Electronic Plans Submission, Review and Storage

William Galloway
CPM Class of 2009

Electronic Sprinkler Plans Submission, Plan Review
and
Data Storage Project

PROBLEM STATEMENT

The Office of State Fire Marshal is located in the SC Department of Labor, Licensing and Regulation (LLR) within the Division of Fire and Life Safety. The Office of State Fire Marshal (OSFM) is charged with the responsibility of reviewing fire protection sprinkler system plans throughout the entire state. This statutory responsibility comes from the Fire Protection Sprinkler Systems Act, §40-10-240, §40-10-250, and §40-10-260. The Fire Protection Sprinkler Systems Act is administered by the Contractor's Licensing Board which is part of LLR. During fiscal year 2008, the OSFM reviewed 2,436 fire protection sprinkler system plans. This is an increase of 9 percent from fiscal year 2007. During fiscal year 2008 over 47 million square feet of sprinklered facilities were reviewed while during fiscal year 2007 the total accounted for just over 31 million square feet. This was an increase of 34 percent in square footage reviewed over the previous year.

Unlike local jurisdictions, the OSFM does not have the ability to charge for plan review services. Previous editions of the Fire Protection Sprinkler Systems Act allowed the OSFM the ability to charge 1 cent per square foot for each square foot of plan reviewed. This change in the statute also required that all fire protection sprinkler system plans are to be reviewed by the OSFM and a letter issued or the plans are considered approved as submitted. The elimination of the ability to charge for fire protection sprinkler system plan reviews and the adoption of a 30 day timeframe for reviews to occur

have meant that many reviews have waited until the last week to get a review before a letter is issued. Currently, the average number of days to turn around a sprinkler project is twenty one (21). The average number of days required for plan review varies however with the growing and slowing demands for construction.

The current process for receiving and reviewing plans by the OSFM is dated and has not kept up with changing technology and increasing customer expectations. These expectations include faster turnaround times for plan review services; electronic plan review services; electronic submission; e-mail notification of plan approvals and cost savings. Therefore, the process needs to be changed. The purpose of this project is to identify the technology available to assist in making the process of receiving, reviewing and storing fire protection sprinkler system plans easier, faster, less expensive, and more efficient. Having the plans submitted electronically will provide the engineering staff with additional working days to review plans if necessary during busy times.

In an effort to improve services and reduce response time, we have developed an electronic submission and review process where documents are sent instantly as e-mail attachments. There are no printing costs for the customer, nor is there any cost for mailing or shipping the documents to the OSFM for review. There is no time lost for shipping the documents to the office as this transmission is completed instantly. The OSFM employs five full-time engineers to conduct plan reviews, but these reviews consist of more than just fire protection sprinkler systems. The OSFM is also statutorily or contractually obligated to conduct other types of reviews. These reviews include: all propane systems, FM – 200 systems (clean agent fire protection systems), aboveground storage tanks at service stations, local detention center buildings, group homes, Department of Disability

and Special Needs facilities, and all state prison building facilities. In addition, the OSFM receives requests for reviews from local jurisdictions with difficult plan reviews on local facilities. Reviews are conducted in the order in which they are received.

DATA COLLECTION

An analysis of other state and local governmental agencies involved with using some form of electronic plan review, submission and/or data storage was reviewed and key individuals with those agencies were contacted. This information was compiled and shared with the engineering staff at weekly meetings and decisions were made by all as to the best direction to go given the information. A meeting was held with the South Carolina Fire Sprinkler Association to see if there was a desire for this type of service and the association was overwhelmingly supportive of the project. After the meeting with the Sprinkler Association it was decided to enlist the services of a private on-line survey instrument that would survey our fire sprinkler contractors and engineers. The purpose of the survey was to determine the file sizes expected to be transmitted what software the customers are using, the customers' ability to transmit plans electronically, and determine the needs the OSFM would have with regard to hardware and software. The survey consisted of 9 multiple choice and two open-ended questions. When the survey began, staff members had to call, e-mail and speak to the sprinkler association numerous times in an effort to get the surveys completed. While everyone we spoke to stated that they were all for the process and could not wait for it to begin, it appeared that few were willing to

take the time to complete the survey to assist in the data collection we needed. Currently we deal with over 100 different fire sprinkler contractors and engineers that submit fire protection sprinkler system plans to our office and only 47 surveys were eventually completed (Appendix F).

DATA ANALYSIS

Preliminary data analysis was accomplished using the private on-line survey data obtained from the 47 surveys previously mentioned. These surveys revealed the following information:

1. 72.4 percent of the respondents use AutoCAD as a design medium, 19.1 percent use Hydracad, 4.3 percent use Micro Station, 2.1 percent use Adobe, and 2.1 percent use Revit.
2. When asked if the customers had the ability to save their files as a .dwg or .dwf file extension, 93.6 percent responded that they could save their files as a .dwg while 79.5 percent responded that they could save their files as a .dwf file extension. Three respondents skipped the question and did not respond.
3. 32.6 percent of the respondents stated that 20 megabytes is the largest file size they have ever produced for fire sprinkler systems; however, 4.2 percent of the respondents stated that over 100 megabytes were needed to properly address the largest file size needed and 18.6 of the respondents stated that 30 megabytes were needed to adequately address the largest file size needed for file transmission.

4. 89.1 percent of the respondents are capable of using a file compression software to decrease the size of a transmission while 10.9 percent do not use any type of compression software. Most respondents use WinZip as their preferred compression software while a minority of the respondents stated that they use PK Zip or Blue Beam.
5. When asked if they have the ability to transmit and receive sprinkler plans electronically, 97.9 percent of the respondents stated that they did while 2.1 percent of the respondents stated that they do not have the ability to transmit plans electronically. 84.4 percent stated that they have the ability to transmit plans with electronic seals while 15.6 percent stated that they cannot transmit electronic plans with the electronic seals. 4.3 percent or two respondents skipped the questions and did not respond at all.
6. When asked if the respondents have the ability to transmit and receive sprinkler plans electronically with electronic signatures, 75 percent of the respondents stated that they had the ability, 25 percent of the respondents stated that they did not have the ability to submit electronic signatures while three of the respondents being surveyed skipped the question and did not respond to the survey question.
7. When asked if they would like our office to offer reviews of electronically submitted documents rather than paper documents; 91.3 percent of the respondents stated that they wanted the OSFM to offer this service while 8.7 percent of the respondents responded that they did not want this service

offered. One respondent skipped the question and did not respond to the survey question.

8. The last survey question asked the respondents if they had any suggestions for the OSFM on this process. Many of the responses were none or N/A while numerous responses were asking us to look at Adobe Professional as an additional option. Still others offered assistance if needed, while a couple did expressed concern at making this process mandatory.

In order to submit fire sprinkler plans electronically it was necessary to first gain an understanding about the law regarding electronic signatures and electronic plans submission. Act 279 of the 2004 session of the South Carolina General Assembly created the Uniform Electronic Transactions Act (Appendix A). That Act required the Budget and Control Board to set up guidelines and standards for electronic signatures and their analysis (Appendix B & C). Although the guidelines and standards did not create any obstacles to this project, the biggest problem with the act was getting the design professionals to understand how to attach their seals and signatures electronically to their plans. In an effort to gain a clearer understanding of how the process of electronic plans submission, plans review and data storage needs to work, it was necessary to first understand how the current plan review process works. This meant creating a process flow list and flowchart of the current review process (Appendix D). It was also necessary to flowchart the proposed electronic submission and review process in order to gain an understanding of the proposed process and see if there was any benefit or savings in time or money to the process (Appendix E). To complete this, a consensus process was used

with the engineering staff to develop a new electronic submission and review process and to field test it and tweak it after a few trial submissions. Each time a set of plans has been received electronically, the reviewing engineer would keep detailed notes as to the process; did it work as it was set up and agreed to or did adjustments need to be made; timeframes for each step in the process were documented and any problems encountered so that we could all meet as a staff and discuss the process and ways to improve or overcome the issues. The staff discovered several things about the new electronic review process: 1) no one size fits all; 2) adjustments will have to be made as issues arise, and 3) reviewing plans electronically is not as difficult as they originally thought.

The OSFM currently uses the fire inspection software CodePal to complete all of its inspections electronically in the field. The software has been effectively used for nearly three years on the inspection side of the OSFM. This software had to be modified by the software vendor in order to be adapted to the engineering side of the office. The software vendor worked with our office to capture all of the data that we currently collect on engineering plan reviews and ensure that it is placed into user friendly forms. This would ensure that the engineering staff would be able to utilize the software with relative ease and in the same manner that the inspection staff does. The use of CodePal on the engineering side of the office will allow for more data to be tracked and more importantly for the data to be available more quickly. Currently, the data we obtain for reports from the engineering database takes several hours to several days to obtain and utilizes valuable staff time. With CodePal the information takes seconds and the data is more user-friendly. Switching the engineering section to CodePal also has the added benefit of allowing steps to be removed from the electronic review process in that the violations are already

preloaded. As the assigned engineer reviews a set of plans he can pull the preloaded violation up in CodePal and add it to the letter to go to the design professional. These preloaded violations will save numerous steps and more importantly, time in the review process.

IMPLEMENTATION PLAN

The implementation team consisted of engineering staff members David Blackwell, Andrew Tharin, Jamie Campbell, Dianne Childress, Kevin King, and Bruce Kritz; Chuck Combs, Joe Naylor, Matt Faile, Matt Gilmore and Alice Davis, Office of Information Services; and William Galloway, Assistant State Fire Marshal, Engineering – Enforcement.

The key components identified in the implementation process consisted of: 1) Hardware and Software needs; 2) Criteria for electronic submission; 3) Separate e-mail account for e-mailing electronic plans; 4) Set up user name and passwords for each customer; 5) Set up folders for each customer to pick up mail and letters off web-site; 6) Advertisement.

1) Hardware and Software needs

Given the status and age of the existing computers that the engineering staff has, there was no doubt that we would not have the capability to conduct electronic reviews using our existing hardware. Research was conducted by the engineering staff with the assistance of the Office of Information Systems (OIS) to determine what systems were

best for conducting electronic plan reviews, and also capable of handling the software and graphics issues that would be required. The engineering staff first looked at what software needs the office would require. This was completed by looking at what other jurisdictions are doing in the electronic plan review arena. Our staff consulted with other jurisdictions that have tried electronic plan review, are in the process of setting up an electronic plan review process or have a process established and is working well for them. Each jurisdiction had some similarities, yet all had vast differences in their processes. After a thorough review, it was determined by the engineering staff that downloadable software from a national vendor was to be the primary source for all plan reviews, while Adobe Professional would serve to cover the remainder of plans. Based on a national search, this appears to be the national trend. Additionally, according to the survey results from Survey Monkey.com, Autodesk Design Review and Adobe Professional will handle all of the electronic plans that are being developed today. In addition to these two plan review software programs, the inspection software CodePal will also be used as a database manager and to reduce the processing times and steps used in the review process. By using CodePal as the database manager, plans review and processing times are estimated to be reduced to an average of 18 days 2 hours and 54 minutes from the paper submission and review process of 29 days and 4 hours. This is a time savings of 11 days 1 hour and 6 minutes over the paper review process, not to mention the cost savings to the customer and the state. The total cost to the OSFM for this new electronic submission and review process will be approximately $17,225.00.

The OSFM will no longer have to file or store large bulk plans for long periods of time (three years) and then go to the expense of ensuring that they are properly destroyed. The OSFM must document to the State Archives Department every plan and every plan review file that is destroyed. Written documentation must be given to the State Archives Department on the cubic feet of plans that are destroyed each year as well as how many inches of plan review files are destroyed. They will also not have the expense of printing or mailing letters anymore as this will be completed and placed on the database and picked up by the customer at their leisure. The customer will save money in printing costs for plans and shipping costs for Fed-Ex, UPS or the USPS. In meetings with the South Carolina Fire Sprinkler Association, printing plans and overnight mailing of plans to the OSFM is the largest expense they have as a contractor outside of labor and material. If setting up an electronic submission and review process would eliminate those expenses and not delay the review process then the South Carolina Fire Sprinkler Association is very supportive of any move that could help them save money.

2) Criteria for electronic submission

To identify the criteria for electronic submission, the engineering team started by examining what the Engineering Practice Act required or permitted with regard to plan submission. After a brief discussion with the Engineering board administrator, Jan Simpson, it was quickly determined that the general assembly passed the Uniform Electronic Transactions Act in 2004 which permitted the use of electronic signatures and seals on plans. This legislation also provided for the use of electronic plan submission for certain types of plans, but not all types. Next the engineering team determined what the

minimum submission requirements needed to be for electronic plans. In essence, we created a checklist for the design professional in an effort to assist them and ensure that we receive everything we need to conduct a full review in accordance with state law and national consensus standards. (Appendix G)

3) Separate e-mail account for e-mailing electronic plans

After running several trial tests with a couple of customers, it became apparent early on in the process that simply e-mailing the plans to the engineering administrative assistant would not work. Another user-friendly account would have to be set up through OIS. One of the problems encountered was the administrative assistants e-mail account would fill up after just one or two of these trial submittals forcing her to delete everything from her account. In discussing the issue with OIS representatives, the normal file size limitations would be removed on a special account that would only be receiving files for plan reviews from customers that have been given a password to submit to the account. This account will be accessible from the OSFM web-site and will not operate like most normal e-mail accounts.

4) Set up user name and passwords for each customer

It was discussed with the administrators at the OIS how this part of the process should be best implemented. One method discussed was to set the username and password for each customer; the other idea was to allow each customer to apply for their own username and password. Given that not every customer will use the electronic submission, review and data storage system, it was determined by OIS that the best way

for this part of the system to work would be for each customer to apply for an account and a password would be assigned by OIS at the time that they apply to use the electronic system. This password would only be good for a particular project; each submittal would be assigned a separate password to protect the integrity of the database server.

5) Set up folders for each customer to pick up mail and letters off web-site

The next item to deal with was to set up an electronic mailbox account for each customer. Since part of this systems sales pitch is to save money and time for both the customer and the state, electronic mailboxes are needed in order to place the letters, marked up plans and any other information that our office needs to communicate to the customer, rather than mailing the information to them. The customer will be able to go to the OSFM web-page and, using the customer's assigned username and password, be able to access their folder from any computer and download the files that are placed in their folder. It was determined that as each customer applies to use the electronic system, an electronic mailbox will be made on the Web-3000 server. Files that are in each folder will be automatically deleted after 15 days when the project is finalized. This will keep the server from becoming overloaded. Permanent storage of all material will be kept on the CodePal database server.

6) Advertisement

Advertisement will perhaps be the most difficult part of the implementation plan. Since the OSFM cannot make electronic plan submission, review and storage mandatory for all of its fire protection sprinkler system customers, the most that we can do is to advertise the benefits of the process. The administrative and engineering team met and

discussed how to best effectively get the word out to all of the fire protection professionals that submit fire protection sprinkler system plans to our office. It was agreed that a four prong approach was best in getting the word out and getting customers to sign up for the new service; 1) We decided that we would write a letter to explain our new process to the customers inviting them to contact us for their password; 2) Place a brief paragraph at the end of each fire protection sprinkler system plan that we review advertising the new system; 3) Advertise the new system on the OSFM web-site; 4) Prepare and send an e-mail to all customers that currently submit fire protection sprinkler plans to the OSFM for review.

Finally, to assist with promotional opportunities with the sprinkler contractors and engineering professionals, a PowerPoint presentation and training class is being developed to be held at the South Carolina Fire Academy. This class will cover the various requirements, process and guidelines for submitting fire sprinkler plans electronically, as well as discussing the numerous benefits such as time and money savings.

EVALUATION METHOD

Prior to making a commitment to invest in the system and the amount of money that it would require, numerous tests were run using real electronic plan submissions from several sprinkler contractors. It was agreed by the administration early on to purchase one computer and run numerous tests and keep notes on what improvements were needed. As these test plans kept coming in, it was obvious that the same issues were showing up time and again. The biggest issues are missing electronic seals and electronic signatures. The

other items we are seeing during the test phase are the same issues we see on paper plans. These may be wrong seismic information, no seismic information, incomplete plans, wrong hydraulic calculations, incomplete hydraulic calculation, incomplete plan information, and other items. Although checklists are used in the plan review process, electronic plan submissions received to date are no different than the paper submissions that have come in over the years. They have consistently had the same information missing, wrong, or incomplete.

As with any new process, there will be issues that will come up and adjustments will have to be made to address those issues. This was the case with CodePal and it has been working effectively for nearly three years. Since CodePal will be the database manager for the submission, review and data storage project, many of the bugs should already be worked out.

One way to evaluate the effectiveness of the program is to determine the number of customers who use the system and the number of plans that are submitted electronically versus the number of plans that are submitted on paper. A six-month performance report identifying how many customers are utilizing the new electronic plan review process will be submitted to the State Fire Marshal. Included in this report will be the number of plans that were submitted electronically versus the number of plans that were submitted on paper. Also, we will include a list of recommendations on suggested improvements. At the end of the twelve-month period, a final report will be submitted to the State Fire Marshal along with an accounting of all expenditures including purchase orders, invoices, and receipts. The final report will also include a list of how many customers are utilizing the electronic plan review service. Included in this final report will be the total number of

electronic plans reviewed versus the number of paper plans reviewed. Also included will be the actual time reduction associated with the new electronic plan review process versus the old paper submission and review process.

SUMMARY

The overwhelming support from the South Carolina Fire Sprinkler Association to move this project forward as quickly as possible has led to a special funding by the OSFM. There was some apprehension on the part of several of the engineering staff members to embrace this technology at first, but after seeing the technology work on one computer and having the ability to ease into it rather that having it forced on them made a significant difference. Also, involving the engineering staff in the decision making process made a significant difference in the buy-in process. Taking the plan review process from paper review to electronic reviews will potentially reduce the review time by more than 11 days. Thus, the cost to invest in the electronic plan review system is more than worth the cost in view of the improvements in customer service.

The total cost to install all new computers in the engineering section will be approximately $9800.00. The cost to install CodePal on these computers is $6600.00. Adobe Professional costs is $825.00 to install on the computers. While this is a significant financial impact to the agency and division, the savings will be realized in less administrative time filing; reduced mail costs; reduced paper costs; less typing time; and no time spent on purging old plans from the files or filing room.

Appendices

Appendix A – Uniform Electronic Transactions Act

Appendix B – South Carolina Standards for Electronic Signatures

Appendix C – Electronic Signatures Analysis Implementation

Appendix D – Flowchart and Spreadsheet of Current Plan Review Process

Appendix E – Flowchart and Spreadsheet of Electronic Review Process

Appendix F – Electronic Sprinkler Plans Submission Surveys

Appendix G – Letter to Sprinkler Contractors and Engineers

Appendix H – Electronic Plan Review E-Mail Submittal Instructions

(A279, R426, H4720)

AN ACT TO AMEND THE CODE OF LAWS OF SOUTH CAROLINA, 1976, BY ADDING CHAPTER 6 TO TITLE 26 SO AS TO ENACT THE UNIFORM ELECTRONIC TRANSACTIONS ACT, PROVIDING FOR DEFINITIONS, LEGAL EFFECT AND ENFORCEABILITY OF AN ELECTRONIC RECORD AND SIGNATURE, CHANGES OR ERRORS IN TRANSMISSION OF AN ELECTRONIC RECORD, COMPLIANCE OF AN ELECTRONIC RECORD OR SIGNATURE WITH OTHER LAWS AFFECTING VALIDITY OR RETENTION OR RECEIPT OF A RECORD OR SIGNATURE, USE OF ELECTRONIC RECORDS BY GOVERNMENTAL AGENCIES, PROMULGATION OF REGULATIONS BY THE BUDGET AND CONTROL BOARD TO ENHANCE THE UTILIZATION OF ELECTRONIC RECORDS AND SIGNATURES, DEVELOPMENT BY THE SECRETARY OF STATE OF MODEL PROCEDURES AND PROMULGATION OF REGULATIONS FOR SECURE ELECTRONIC TRANSACTIONS, INCLUDING LICENSING OF THIRD PARTIES, AND TO PROVIDE FOR THE USE OF THE ELECTRONIC POSTMARK TO PERFECT SERVICE OF PROCESS IN A MANNER PRESCRIBED BY THE STATE SUPREME COURT AND IN THE OPERATIONS OF STATE AGENCIES AS PRESCRIBED BY THE BUDGET AND CONTROL BOARD; TO MAKE THE COMPUTER CRIME ACT APPLICABLE TO THE UNIFORM ELECTRONIC TRANSACTIONS ACT; AND TO REPEAL CHAPTER 5 OF TITLE 26, THE SOUTH CAROLINA ELECTRONIC COMMERCE ACT.

Be it enacted by the General Assembly of the State of South Carolina:

Uniform Electronic Transactions Act

SECTION 1. Title 26 of the 1976 Code is amended by adding:

"CHAPTER 6

Uniform Electronic Transactions Act

Section 26-6-10. (A) This chapter may be cited as the 'Uniform Electronic Transactions Act'.

South Carolina General Assembly
115th Session, 2003-2004

A279, R426, H4720

STATUS INFORMATION

General Bill
Sponsors: Rep. Harrison
Document Path: l:\council\bills\ms\7061mm04.doc
Companion/Similar bill(s): 908

Introduced in the House on February 10, 2004
Introduced in the Senate on March 9, 2004
Last Amended on June 1, 2004
Passed by the General Assembly on June 2, 2004
Governor's Action: July 16, 2004, Signed

Summary: Uniform Electronic Transactions Act

HISTORY OF LEGISLATIVE ACTIONS

Date	Body	Action Description with journal page number
2/10/2004	House	Introduced and read first time HJ-8
2/10/2004	House	Referred to Committee on **Judiciary** HJ-8
2/25/2004	House	Committee report: Favorable with amendment **Judiciary** HJ-6
2/26/2004		Scrivener's error corrected
3/3/2004	House	Amended HJ-20
3/3/2004	House	Read second time HJ-20
3/4/2004	House	Read third time and sent to Senate HJ-19
3/4/2004		Scrivener's error corrected
3/9/2004	Senate	Introduced and read first time SJ-16
3/9/2004	Senate	Referred to Committee on **Judiciary** SJ-16
5/12/2004	Senate	Committee report: Favorable with amendment **Judiciary** SJ-21
5/13/2004	Senate	Amended SJ-27
5/19/2004	Senate	Amended SJ-56
5/19/2004	Senate	Read second time SJ-56
5/19/2004	Senate	Ordered to third reading with notice of amendments SJ-56
5/20/2004	Senate	Read third time and returned to House with amendments SJ-19
5/26/2004	House	Debate adjourned until Thursday, May 27, 2004 HJ-53
5/27/2004	House	Debate adjourned until Tuesday, June 1, 2004
6/1/2004	House	Senate amendment amended HJ-28
6/1/2004	House	Returned to Senate with amendments HJ-30
6/2/2004	Senate	Concurred in House amendment and enrolled SJ-37
6/3/2004		Ratified R 426
7/16/2004		Signed By Governor
7/26/2004		Copies available
7/26/2004		Effective date 07/16/04
7/28/2004		Act No. 279

View the latest legislative information at the LPITS web site

(B) Consistent with the provisions of the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. Section 7002(a), this chapter provides alternative procedures or requirements for the use of electronic records to establish the legal effect or validity of records in electronic transactions.

Section 26-6-20. As used in this chapter:

(1) 'Agreement' means the bargain of the parties in fact, as found in their language or inferred from other circumstances and from rules, regulations, and procedures giving the effect of agreements under law otherwise applicable to a particular transaction.

(2) 'Automated transaction' means a transaction conducted or performed, in whole or in part, by electronic means or electronic records, in which the acts or records of any of the parties are not reviewed by an individual in the ordinary course in forming a contract, performing under an existing contract, or fulfilling an obligation required by the transaction.

(3) 'Computer program' means a set of statements or instructions used directly or indirectly in an information processing system to bring about a certain result.

(4) 'Contract' means the total legal obligation resulting from the agreement of the parties as affected by this chapter and other applicable law.

(5) 'Electronic' means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(6) 'Electronic agent' means a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual.

(7) 'Electronic record' means a record created, generated, sent, communicated, received, or stored by electronic means.

(8) 'Electronic signature' means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

(9) 'Governmental agency' means an executive, legislative, or judicial agency, department, board, commission, authority, institution, or instrumentality of the federal government or of a state or of a county, municipality, or other political subdivision of a state.

(10) 'Individual' means a single natural person; one human being.

(11) 'Information' means data, text, images, sounds, codes, computer programs, software, databases, or other forms for the communication or reception of knowledge.

(12) 'Information processing system' means an electronic system for creating, generating, sending, receiving, storing, displaying, or processing information.

(13) 'Person' means an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation, or other legal or commercial entity.

(14) 'Record' means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

(15) 'Security procedure' means a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures.

(16) 'State' means a state of the United States, the District of Columbia, Puerto Rico, the United States Virgin Islands, or any territory or insular possession subject to the jurisdiction of the United States. The term includes an Indian tribe or band, or Alaskan native village, which is recognized by federal law or formally acknowledged by a state.

(17) 'Transaction' means an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.

(18) 'United States Postal Service Electronic Postmark' means an electronic service provided by the United States Postal Service that provides evidentiary proof that an electronic document existed in a certain form at a certain time and the electronic document was opened or the contents of the electronic document were displayed at a time and date documented by the United States Post Office.

Section 26-6-30. (A) Except as otherwise provided in subsection (B), this chapter applies to electronic records and electronic signatures relating to a transaction.

(B) This chapter does not apply to a transaction:

(1) in connection with an order for prescription drugs; or

(2) to the extent the transaction is governed by:

(a) a law governing the creation and execution of wills, codicils, or testamentary trusts;

(b) the Uniform Commercial Code, other than Sections 36-1-107 and 36-1-206, Chapter 2 of Title 36, and Chapter 2A of Title 36; or

(c) the Electronic Signatures in Global and National Commerce Act, 114 Stat. 464, 15 U.S.C. at 7001 et seq., but it is not intended to limit, modify, or supersede Section 101(c) of the act, and to the extent that the notices exempted below are excluded from the scope of the Electronic Signatures in Global and National Commerce Act, 114 Stat. 464, 15 U.S.C. at 7003, this chapter of Title 26 does not apply to a notice required by law regarding:

(i) the cancellation or termination of utility services (including water, heat, and power);

(ii) default, acceleration, repossession, foreclosure, eviction, or the right to cure under a credit agreement secured by a primary residence of an individual or a rental agreement for a primary residence of an individual;

(iii) the cancellation or termination of health insurance or benefits or life insurance benefits, excluding annuities;

(iv) the recall of a product or material failure of a product, that risks endangering health or safety; or

(v) a law requiring a document to accompany any transportation or handling of hazardous materials, pesticides, or other toxic or dangerous materials.

(C) This chapter applies to an electronic record or electronic signature otherwise excluded from the application of the chapter pursuant to subsection (B) to the extent it is governed by a law other than those specified in subsection (B).

(D) A transaction subject to this chapter is also subject to other applicable substantive law.

Section 26-6-40. This chapter applies to an electronic record or electronic signature created, generated, sent, communicated, received, or stored on or after the effective date of this chapter.

Section 26-6-50. (A) This chapter does not require a record or signature to be created, generated, sent, communicated, received, stored, or otherwise processed or used by electronic means or in electronic form.

(B) This chapter applies only to transactions between parties who agree to conduct transactions by electronic means. Whether the parties agree to conduct a transaction by electronic means is determined from the context and surrounding circumstances, including the conduct of the parties.

(C) A party that agrees to conduct a transaction by electronic means may refuse to conduct other transactions by electronic means. This right of refusal shall not be waived by agreement.

(D) Except as otherwise provided in this chapter, the effect of its provisions may be varied by agreement. The presence in certain provisions of this chapter of the words 'unless otherwise agreed', or words of similar import, does not imply that the effect of other provisions may not be varied by agreement.

(E) Whether an electronic record or electronic signature has legal consequences is determined by this chapter and other applicable laws.

Section 26-6-60. This chapter must be construed and applied to:

(1) facilitate electronic transactions consistent with other applicable law;

(2) be consistent with reasonable practice concerning electronic transactions and with continued expansion of those practices; and

(3) effectuate its general purpose to make uniform the law with respect to the subject of this chapter among states enacting it.

Section 26-6-70. (A) A record or signature must not be denied legal effect or enforceability solely because it is in electronic form.

(B) A contract must not be denied legal effect or enforceability solely because an electronic record is used in its formation.

(C) An electronic record satisfies a law requiring a record to be in writing.

(D) An electronic signature satisfies a law requiring a signature.

Section 26-6-80. (A) If parties agree to conduct a transaction by electronic means and a law requires a person to provide, send, or deliver information in writing to another person, the requirement is satisfied if the information is provided, sent, or delivered in an electronic record capable of retention by the recipient at the time of receipt. An electronic record is not capable of retention by the recipient if the sender or its information processing system inhibits the ability of the recipient to print or store the electronic record.

(B) If another provision of law requires a record to be posed or displayed in a certain manner, be sent, communicated, or transmitted by a specified method, or contain information formatted in a certain manner, the record must:

(1) be posted or displayed in the manner specified in the other law;

(2) be sent, communicated, or transmitted by the method specified in the other law, except as otherwise provided in subsection (D)(2); and

(3) contain the information formatted in the manner specified in the other law.

(C) The electronic record is not enforceable against the recipient if a sender inhibits the ability of a recipient to store or print an electronic record.

(D) The requirements of this section shall not be varied by agreement, except that:

(1) to the extent a law other than this chapter requires information to be provided, sent, or delivered in writing but permits that requirement to be varied by agreement, the requirement pursuant to subsection (A) that the information be in the form of an electronic record capable of retention also may be varied by agreement; and

(2) a requirement pursuant to a law other than this chapter to send, communicate, or transmit a record by first-class mail, postage prepaid, or regular United States mail, may be varied by agreement to the extent permitted by the other law.

Section 26-6-90. (A) An electronic record or electronic signature is attributable to a person if it is the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of a security procedure applied to determine the person to which the electronic record or electronic signature was attributable.

(B) The effect of an electronic record or electronic signature attributed to a person pursuant to subsection (A) is determined from the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties' agreement, if any, and as otherwise provided by law.

Section 26-6-100. (A) If a change or error occurs in the transmission of an electronic record between parties to a transaction:

(1) the conforming party may avoid the effect of the changed or erroneous electronic record, if the parties have agreed to use a security procedure to detect changes or errors and one party has conformed to the procedure but the other party has not and the nonconforming party would have detected the change or error had he also conformed;

(2) an individual may avoid the effect of an electronic record that resulted from an error made by the individual in dealing with the electronic agent of another person if the electronic agent did not provide an opportunity for the prevention or correction of the error and, at the time the individual learns of the error, the individual:

(a) promptly notifies the other person of the error and that the individual did not intend to be bound by the electronic record received by the other person;

(b) takes reasonable steps, including steps that conform to the reasonable instructions of the other person, to return or destroy, as instructed, the consideration received as a result of the erroneous electronic record; and

(c) has not used or received any benefit or value from the consideration received from the other person.

(B) If subsection (A) does not apply, the change or error has the effect provided by other law, including the law of mistake, and the parties' contract, if any.

(C) The provisions of subsections (A)(2) and (B) shall not be varied by agreement.

Section 26-6-110. A law requiring a signature or record to be notarized, acknowledged, verified, or made under oath is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable law, is attached to or logically associated with the signature or record.

Section 26-6-120. (A) A law requiring a record to be retained is satisfied by retaining an electronic record of the information that:

(1) accurately reflects the information in the record after it was first generated in its final form as an electronic record or otherwise; and

(2) remains accessible for later reference.

(B) A requirement to retain a record in accordance with subsection (A) does not apply to information whose only purpose is to enable the record to be sent, communicated, or received.

(C) A person may satisfy subsection (A) by using the services of another person if the requirements of that subsection are satisfied otherwise.

(D) A law requiring a record to be presented or retained in its original form, or providing consequences if the record is not presented or retained in its original form, is satisfied by an electronic record retained in accordance with subsection (A).

(E) A law requiring retention of a check is satisfied by retention of an electronic record of the information on the front and back of the check in accordance with subsection (A).

(F) A record retained as an electronic record in accordance with subsection (A) satisfies a law requiring a person to retain a record for evidentiary, audit, or like purposes, unless a law enacted after the

effective date of this chapter specifically prohibits the use of an electronic record for the specified purpose.

(G) This section does not preclude a governmental agency of this State from specifying additional requirements for the retention of a record subject to the agency's jurisdiction.

Section 26-6-130. Evidence of a record or signature may not be excluded in a proceeding solely because the record or signature is in electronic form.

Section 26-6-140. In an automated transaction:

(1) a contract may be formed by the interaction of electronic agents of the parties, even if an individual was not aware of or reviewed the electronic agents' actions or the resulting terms and agreements;

(2) a contract may be formed by the interaction of an electronic agent and an individual, acting on the individual's own behalf or for another person, including by an interaction in which the individual performs actions that the individual is free to refuse to perform and which the individual knows or has reason to know will cause the electronic agent to complete the transaction or performance; and

(3) the terms of the contract are determined by the substantive law applicable to it.

Section 26-6-150. (A) Unless otherwise agreed between the sender and the recipient, an electronic record is sent when it:

(1) is addressed properly or otherwise directed properly to an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record;

(2) is in a form capable of being processed by that system; and

(3) enters an information processing system outside the control of the sender or of a person that sent the electronic record on behalf of the sender or enters a region of the information processing system designated or used by the recipient and under the control of the recipient.

(B) Unless otherwise agreed between a sender and the recipient, an electronic record is received when it:

(1) enters an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record; and

(2) is in a form capable of being processed by that system.

(C) Subsection (B) applies even if the place the information processing system is located is different from the place the electronic record is considered to be received pursuant to subsection (D).

(D) Unless otherwise expressly provided in the electronic record or agreed between the sender and the recipient, an electronic record is considered to be sent from the sender's place of business and to be received at the recipient's place of business. For purposes of this subsection, the place of business is:

(1) the place having the closest relationship to the underlying transaction, if the sender or recipient has more than one place of business; and

(2) the sender's or recipient's residence, if the sender or the recipient does not have a place of business.

(E) An electronic record is received pursuant to subsection (B) even if an individual is not aware of its receipt.

(F) Receipt of an electronic acknowledgment from an information processing system described in subsection (B) establishes that a record was received but is not sufficient to establish that the content sent corresponds to the content received.

(G) If a person is aware that an electronic record purportedly sent pursuant to subsection (A), or purportedly received pursuant to subsection (B), was not actually sent or received, the legal effect of the sending or receipt is determined by other applicable law. Except to the extent permitted by the other law, the requirements of this subsection shall not be varied by agreement.

Section 26-6-160. (A) In this section, 'transferable record' means an electronic record that:

(1) would be a negotiable instrument under Chapter 3 of Title 36 or a document of title under Chapter 7 of Title 36 if the electronic record were in writing; and

(2) the issuer of the electronic record expressly has agreed is a transferable record.

(B) A person has control of a transferable record if a system employed for evidencing the transfer of interests in the transferable record reliably establishes that person as the person to which the transferable record was issued or transferred.

(C) A system satisfies subsection (B), and a person is considered to have control of a transferable record, if the transferable record is created, stored, and assigned in such a manner that:

(1) there exists a single authoritative copy of the transferable record that is unique, identifiable, and, except as otherwise provided in items (4), (5), and (6), unalterable;

(2) the authoritative copy identifies the person asserting control as the person to which the transferable record was:

(a) issued; or

(b) most recently transferred, if the authoritative copy indicates that the transferable record has been transferred;

(3) the authoritative copy is communicated to and maintained by the person asserting control or its designated custodian;

(4) copies or revisions that add or change an identified assignee of the authoritative copy are made only with the consent of the person asserting control;

(5) each copy of the authoritative copy and a copy of a copy are readily identifiable as copies that are not the authoritative copy; and

(6) a revision of the authoritative copy is readily identifiable as authorized or unauthorized.

(D) Except as otherwise agreed, a person having control of a transferable record is the holder, as defined in Section 36-1-201(20), of the transferable record and has the same rights and defenses as a holder of an equivalent record or writing pursuant to Title 36, including the rights and defenses of a holder in due course, a holder to which a negotiable document of title has been duly negotiated, or a purchaser, respectively if the applicable statutory requirements pursuant to Section 36-3-302, 36-7-501, or 36-9-308 are satisfied. Delivery, possession, and endorsement are not required to obtain or exercise the rights pursuant to this subsection.

(E) Except as otherwise agreed, an obligor under a transferable record has the same rights and defenses as an equivalent obligor under equivalent records or writings pursuant to Title 36.

(F) The person seeking to enforce the transferable record shall provide, upon request, reasonable proof that he is in control of the transferable record. Proof may include access to the authoritative copy of the transferable record and related business records sufficient to review the terms of the transferable record and to establish the identity of the person having control of the transferable record.

Section 26-6-170. Each governmental agency of this State shall determine if, and the extent to which, it will create and retain electronic records and convert written records to electronic records.

Section 26-6-180. (A) Each governmental agency of this State shall determine if, and the extent to which, it will send and accept electronic records and electronic signatures to and from other persons and otherwise create, generate, communicate, store, process, use, and rely upon electronic records and electronic signatures.

(B) To the extent that a governmental agency uses electronic records and electronic signatures pursuant to subsection (A), the governmental agency, in consultation with the South Carolina State Budget and Control Board, giving due consideration to security, may specify:

(1) the manner and format in which the electronic records must be created, generated, sent, communicated, received, and stored and the systems established for those purposes;

(2) if electronic records must be signed by electronic means, the type of electronic signature required, the manner and format in which the electronic signature must be affixed to the electronic record, and the identity of, or criteria that must be met by, a third party used by a person filing a document to facilitate the process;

(3) control processes and procedures appropriate to ensure adequate preservation, disposition, integrity, security, confidentiality, and auditability of electronic records; and

(4) other attributes required for electronic records which are specified for corresponding nonelectronic records or reasonably necessary under the circumstances.

(C) Except as otherwise provided in Section 26-6-120, this chapter does not require a governmental agency of this State to use or permit the use of electronic records or electronic signatures.

Section 26-6-190. (A) The South Carolina State Budget and Control Board shall adopt standards to coordinate, create, implement, and facilitate the use of common approaches and technical infrastructure, as appropriate, to enhance the utilization of electronic records, electronic signatures, and security procedures by and for public entities of the State. Local political subdivisions may consent to be governed by these standards.

(B) The Secretary of State may develop, implement, and facilitate the use of model procedures for the use of electronic records, electronic signatures, and security procedures for all other purposes, including private commercial transactions and contracts. The Secretary of State also may promulgate regulations as to methods, means, and standards for secure electronic transactions including administration by the Secretary of State or the licensing of third parties to serve in that capacity, or both.

(C) In accordance with Sections 26-6-20(18) and 26-6-195, and in reference to all South Carolina laws, rules, and regulations pertaining to service of process where service shall be made on entities described in Rule 4(d)(3) of the South Carolina Rules of Civil Procedure, those

entities shall be served under Rule 4(d)(8) of the South Carolina Rules of Civil Procedure by:

(1) registered or certified mail-return receipt requested, addressed to the office of the registered agent;

(2) registered or certified mail-return receipt requested, addressed to the office of the secretary of the corporation at its principal office;

(3) e-mailing the service of process that has been postmarked by a United States Postal Service Electronic Postmark in a manner approved by the South Carolina Supreme Court to an e-mail address registered with the Secretary of State for the corporation; or

(4) e-mailing the service of process that has been postmarked by a United States Postal Service Electronic Postmark in a manner approved by the South Carolina Supreme Court to an e-mail address registered with the Secretary of State for the agent for service of process for the corporation.

Section 26-6-195. Notwithstanding any other provisions in this chapter, a governmental agency may use, in accordance with policies and procedures developed by the South Carolina Budget and Control Board and as circumstances allow, in order to perfect service of process of any communication, an e-mail address from any vendor, entity, or individual the governmental agency regulates or does business with, or an e-mail address from the agent for service of process of that vendor, entity, or individual. Such communication postmarked by a United States Postal Service Electronic Postmark shall have the same force of law as the United States Post Office certified mail-return receipt requested. The South Carolina Budget and Control Board shall devise policies and procedures for the use of the United States Postal Service Electronic Postmark in respect to state agencies and operations. These policies and procedures, where necessary, must consider the persons or entities which do not have an e-mail address.

Section 26-6-210. The Computer Crime Act, as contained in Chapter 16 of Title 16, is expressly made applicable to and incorporated into this chapter."

Repeal

SECTION 2. Chapter 5 of Title 26 of the 1976 Code is repealed.

Severability

SECTION 3. If a provision of this chapter or its application to a person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this chapter which can be given effect without the invalid provision or application, and to this end the provisions of this chapter are severable.

Time effective

SECTION 4. This act takes effect upon approval by the Governor.

Ratified the 3rd day of June, 2004.

Approved the 16th day of July, 2004.

DISCLAIMER

The South Carolina Legislative Council is offering access to the unannotated South Carolina Code of Laws on the Internet as a service to the public. The unannotated South Carolina Code on the General Assembly's website is now current through the 2007 regular session. The unannotated South Carolina Code, consisting only of Code text and numbering, may be copied from this website at the reader's expense and effort without need for permission.

The Legislative Council is unable to assist users of this service with legal questions. Also, legislative staff cannot respond to requests for legal advice or the application of the law to specific facts. Therefore, to understand and protect your legal rights, you should consult your own private lawyer regarding all legal questions.

While every effort was made to ensure the accuracy and completeness of the unannotated South Carolina Code available on the South Carolina General Assembly's website, the unannotated South Carolina Code is not official, and the state agencies preparing this website and the General Assembly are not responsible for any errors or omissions which may occur in these files. Only the current published volumes of the South Carolina Code of Laws Annotated and any pertinent acts and joint resolutions contain the official version.

Please note that the Legislative Council is not able to respond to individual inquiries regarding research or the features, format, or use of this website. However, you may notify Legislative Printing, Information and Technology Systems at LPITS@scstatehouse.net regarding any apparent errors or omissions in content of Code sections on this website, in which case LPITS will relay the information to appropriate staff members of the South Carolina Legislative Council for investigation.

CHAPTER 6.

UNIFORM ELECTRONIC TRANSACTIONS ACT

SECTION 26-6-10. Short title; purpose.

(A) This chapter may be cited as the "Uniform Electronic Transactions Act".
(B) Consistent with the provisions of the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. Section 7002(a), this chapter provides alternative procedures or requirements for the use of electronic records to establish the legal effect or validity of records in electronic transactions.

SECTION 26-6-20. Definitions.

As used in this chapter:
(1) "Agreement" means the bargain of the parties in fact, as found in their language or inferred from other circumstances and from rules, regulations, and procedures giving the effect of agreements under law otherwise applicable to a particular transaction.
(2) "Automated transaction" means a transaction conducted or performed, in whole or in part, by electronic means or electronic records, in which the acts or records of any of the parties are not reviewed by an individual in the ordinary course in forming a contract, performing under an existing contract, or fulfilling an obligation required by the transaction.
(3) "Computer program" means a set of statements or instructions used directly or indirectly in an information processing system to bring about a certain result.
(4) "Contract" means the total legal obligation resulting from the agreement of the parties as affected by this chapter and other applicable law.
(5) "Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.
(6) "Electronic agent" means a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual.
(7) "Electronic record" means a record created, generated, sent, communicated, received, or stored by electronic means.
(8) "Electronic signature" means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.
(9) "Governmental agency" means an executive, legislative, or judicial agency, department, board, commission, authority, institution, or instrumentality of the federal government or of a state or of a county, municipality, or other political subdivision of a state.
(10) "Individual" means a single natural person; one human being.
(11) "Information" means data, text, images, sounds, codes, computer programs, software, databases, or other forms for the communication or reception of knowledge.
(12) "Information processing system" means an electronic system for creating, generating, sending, receiving, storing, displaying, or processing information.
(13) "Person" means an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation, or other legal or commercial entity.
(14) "Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.
(15) "Security procedure" means a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures.

(16) "State" means a state of the United States, the District of Columbia, Puerto Rico, the United States Virgin Islands, or any territory or insular possession subject to the jurisdiction of the United States. The term includes an Indian tribe or band, or Alaskan native village, which is recognized by federal law or formally acknowledged by a state.
(17) "Transaction" means an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.
(18) "United States Postal Service Electronic Postmark" means an electronic service provided by the United States Postal Service that provides evidentiary proof that an electronic document existed in a certain form at a certain time and the electronic document was opened or the contents of the electronic document were displayed at a time and date documented by the United States Post Office.

SECTION 26-6-30. Applicability to electronic records and electronic signatures relating to transaction; exceptions.

(A) Except as otherwise provided in subsection (B), this chapter applies to electronic records and electronic signatures relating to a transaction.
(B) This chapter does not apply to a transaction:
(1) in connection with an order for prescription drugs; or
(2) to the extent the transaction is governed by:
(a) a law governing the creation and execution of wills, codicils, or testamentary trusts;
(b) the Uniform Commercial Code, other than Sections 36-1-107 and 36-1-206, Chapter 2 of Title 36, and Chapter 2A of Title 36; or
(c) the Electronic Signatures in Global and National Commerce Act, 114 Stat. 464, 15 U.S.C. at 7001 et seq., but it is not intended to limit, modify, or supersede Section 101(c) of the act, and to the extent that the notices exempted below are excluded from the scope of the Electronic Signatures in Global and National Commerce Act, 114 Stat. 464, 15 U.S.C. at 7003, this chapter of Title 26 does not apply to a notice required by law regarding:
(i) the cancellation or termination of utility services (including water, heat, and power);
(ii) default, acceleration, repossession, foreclosure, eviction, or the right to cure under a credit agreement secured by a primary residence of an individual or a rental agreement for a primary residence of an individual;
(iii) the cancellation or termination of health insurance or benefits or life insurance benefits, excluding annuities;
(iv) the recall of a product or material failure of a product, that risks endangering health or safety; or
(v) a law requiring a document to accompany any transportation or handling of hazardous materials, pesticides, or other toxic or dangerous materials.
(C) This chapter applies to an electronic record or electronic signature otherwise excluded from the application of the chapter pursuant to subsection (B) to the extent it is governed by a law other than those specified in subsection (B).
(D) A transaction subject to this chapter is also subject to other applicable substantive law.

SECTION 26-6-40. Prospective application of chapter.

This chapter applies to an electronic record or electronic signature created, generated, sent, communicated, received, or stored on or after the effective date of this chapter.

SECTION 26-6-50. Agreement of parties to conduct transactions by electronic means.

(A) This chapter does not require a record or signature to be created, generated, sent, communicated, received, stored, or otherwise processed or used by electronic means or in electronic form.
(B) This chapter applies only to transactions between parties who agree to conduct transactions by

electronic means. Whether the parties agree to conduct a transaction by electronic means is determined from the context and surrounding circumstances, including the conduct of the parties.
(C) A party that agrees to conduct a transaction by electronic means may refuse to conduct other transactions by electronic means. This right of refusal shall not be waived by agreement.
(D) Except as otherwise provided in this chapter, the effect of its provisions may be varied by agreement. The presence in certain provisions of this chapter of the words "unless otherwise agreed", or words of similar import, does not imply that the effect of other provisions may not be varied by agreement.
(E) Whether an electronic record or electronic signature has legal consequences is determined by this chapter and other applicable laws.

SECTION 26-6-60. Construction and application.

This chapter must be construed and applied to:
(1) facilitate electronic transactions consistent with other applicable law;
(2) be consistent with reasonable practice concerning electronic transactions and with continued expansion of those practices; and
(3) effectuate its general purpose to make uniform the law with respect to the subject of this chapter among states enacting it.

SECTION 26-6-70. Legality of electronic contracts, records, and signatures.

(A) A record or signature must not be denied legal effect or enforceability solely because it is in electronic form.
(B) A contract must not be denied legal effect or enforceability solely because an electronic record is used in its formation.
(C) An electronic record satisfies a law requiring a record to be in writing.
(D) An electronic signature satisfies a law requiring a signature.

SECTION 26-6-80. Satisfying requirement that information be in writing; complying with manner of transmission and format requirements; exceptions.

(A) If parties agree to conduct a transaction by electronic means and a law requires a person to provide, send, or deliver information in writing to another person, the requirement is satisfied if the information is provided, sent, or delivered in an electronic record capable of retention by the recipient at the time of receipt. An electronic record is not capable of retention by the recipient if the sender or its information processing system inhibits the ability of the recipient to print or store the electronic record.
(B) If another provision of law requires a record to be posed or displayed in a certain manner, be sent, communicated, or transmitted by a specified method, or contain information formatted in a certain manner, the record must:
(1) be posted or displayed in the manner specified in the other law;
(2) be sent, communicated, or transmitted by the method specified in the other law, except as otherwise provided in subsection (D)(2); and
(3) contain the information formatted in the manner specified in the other law.
(C) The electronic record is not enforceable against the recipient if a sender inhibits the ability of a recipient to store or print an electronic record.
(D) The requirements of this section shall not be varied by agreement, except that:
(1) to the extent a law other than this chapter requires information to be provided, sent, or delivered in writing but permits that requirement to be varied by agreement, the requirement pursuant to subsection (A) that the information be in the form of an electronic record capable of retention also may be varied by agreement; and
(2) a requirement pursuant to a law other than this chapter to send, communicate, or transmit a record by

first-class mail, postage prepaid, or regular United States mail, may be varied by agreement to the extent permitted by the other law.

SECTION 26-6-90. Showing that electronic record or signature is attributable to a person; effect of electronic record or signature.

(A) An electronic record or electronic signature is attributable to a person if it is the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of a security procedure applied to determine the person to which the electronic record or electronic signature was attributable.
(B) The effect of an electronic record or electronic signature attributed to a person pursuant to subsection (A) is determined from the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties' agreement, if any, and as otherwise provided by law.

SECTION 26-6-100. Change or error in transmission of electronic record; circumstances under which effect may be avoided; applicability of other law.

(A) If a change or error occurs in the transmission of an electronic record between parties to a transaction:
(1) the conforming party may avoid the effect of the changed or erroneous electronic record, if the parties have agreed to use a security procedure to detect changes or errors and one party has conformed to the procedure but the other party has not and the nonconforming party would have detected the change or error had he also conformed;
(2) an individual may avoid the effect of an electronic record that resulted from an error made by the individual in dealing with the electronic agent of another person if the electronic agent did not provide an opportunity for the prevention or correction of the error and, at the time the individual learns of the error, the individual:
(a) promptly notifies the other person of the error and that the individual did not intend to be bound by the electronic record received by the other person;
(b) takes reasonable steps, including steps that conform to the reasonable instructions of the other person, to return or destroy, as instructed, the consideration received as a result of the erroneous electronic record; and
(c) has not used or received any benefit or value from the consideration received from the other person.
(B) If subsection (A) does not apply, the change or error has the effect provided by other law, including the law of mistake, and the parties' contract, if any.
(C) The provisions of subsections (A)(2) and (B) shall not be varied by agreement.

SECTION 26-6-110. Satisfying requirement that signature or record be notarized.

A law requiring a signature or record to be notarized, acknowledged, verified, or made under oath is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable law, is attached to or logically associated with the signature or record.

SECTION 26-6-120. Satisfying law requiring a record to be maintained; checks.

(A) A law requiring a record to be retained is satisfied by retaining an electronic record of the information that:
(1) accurately reflects the information in the record after it was first generated in its final form as an electronic record or otherwise; and
(2) remains accessible for later reference.

(B) A requirement to retain a record in accordance with subsection (A) does not apply to information whose only purpose is to enable the record to be sent, communicated, or received.
(C) A person may satisfy subsection (A) by using the services of another person if the requirements of that subsection are satisfied otherwise.
(D) A law requiring a record to be presented or retained in its original form, or providing consequences if the record is not presented or retained in its original form, is satisfied by an electronic record retained in accordance with subsection (A).
(E) A law requiring retention of a check is satisfied by retention of an electronic record of the information on the front and back of the check in accordance with subsection (A).
(F) A record retained as an electronic record in accordance with subsection (A) satisfies a law requiring a person to retain a record for evidentiary, audit, or like purposes, unless a law enacted after the effective date of this chapter specifically prohibits the use of an electronic record for the specified purpose.
(G) This section does not preclude a governmental agency of this State from specifying additional requirements for the retention of a record subject to the agency's jurisdiction.

SECTION 26-6-130. Admissibility as evidence.

Evidence of a record or signature may not be excluded in a proceeding solely because the record or signature is in electronic form.

SECTION 26-6-140. Automated transactions; formation of contract.

In an automated transaction:
(1) a contract may be formed by the interaction of electronic agents of the parties, even if an individual was not aware of or reviewed the electronic agents' actions or the resulting terms and agreements;
(2) a contract may be formed by the interaction of an electronic agent and an individual, acting on the individual's own behalf or for another person, including by an interaction in which the individual performs actions that the individual is free to refuse to perform and which the individual knows or has reason to know will cause the electronic agent to complete the transaction or performance; and
(3) the terms of the contract are determined by the substantive law applicable to it.

SECTION 26-6-150. When electronic record sent and received.

(A) Unless otherwise agreed between the sender and the recipient, an electronic record is sent when it:
(1) is addressed properly or otherwise directed properly to an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record;
(2) is in a form capable of being processed by that system; and
(3) enters an information processing system outside the control of the sender or of a person that sent the electronic record on behalf of the sender or enters a region of the information processing system designated or used by the recipient and under the control of the recipient.
(B) Unless otherwise agreed between a sender and the recipient, an electronic record is received when it:
(1) enters an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record; and
(2) is in a form capable of being processed by that system.
(C) Subsection (B) applies even if the place the information processing system is located is different from the place the electronic record is considered to be received pursuant to subsection (D).
(D) Unless otherwise expressly provided in the electronic record or agreed between the sender and the recipient, an electronic record is considered to be sent from the sender's place of business and to be received at the recipient's place of business. For purposes of this subsection, the place of business is:

(1) the place having the closest relationship to the underlying transaction, if the sender or recipient has more than one place of business; and
(2) the sender's or recipient's residence, if the sender or the recipient does not have a place of business.
(E) An electronic record is received pursuant to subsection (B) even if an individual is not aware of its receipt.
(F) Receipt of an electronic acknowledgment from an information processing system described in subsection (B) establishes that a record was received but is not sufficient to establish that the content sent corresponds to the content received.
(G) If a person is aware that an electronic record purportedly sent pursuant to subsection (A), or purportedly received pursuant to subsection (B), was not actually sent or received, the legal effect of the sending or receipt is determined by other applicable law. Except to the extent permitted by the other law, the requirements of this subsection shall not be varied by agreement.

SECTION 26-6-160. Establishing person as having control of transferable record; rights and defenses; proof of control.

(A) In this section, "transferable record" means an electronic record that:
(1) would be a negotiable instrument under Chapter 3 of Title 36 or a document of title under Chapter 7 of Title 36 if the electronic record were in writing; and
(2) the issuer of the electronic record expressly has agreed is a transferable record.
(B) A person has control of a transferable record if a system employed for evidencing the transfer of interests in the transferable record reliably establishes that person as the person to which the transferable record was issued or transferred.
(C) A system satisfies subsection (B), and a person is considered to have control of a transferable record, if the transferable record is created, stored, and assigned in such a manner that:
(1) there exists a single authoritative copy of the transferable record that is unique, identifiable, and, except as otherwise provided in items (4), (5), and (6), unalterable;
(2) the authoritative copy identifies the person asserting control as the person to which the transferable record was:
(a) issued; or
(b) most recently transferred, if the authoritative copy indicates that the transferable record has been transferred;
(3) the authoritative copy is communicated to and maintained by the person asserting control or its designated custodian;
(4) copies or revisions that add or change an identified assignee of the authoritative copy are made only with the consent of the person asserting control;
(5) each copy of the authoritative copy and a copy of a copy are readily identifiable as copies that are not the authoritative copy; and
(6) a revision of the authoritative copy is readily identifiable as authorized or unauthorized.
(D) Except as otherwise agreed, a person having control of a transferable record is the holder, as defined in Section 36-1-201(20), of the transferable record and has the same rights and defenses as a holder of an equivalent record or writing pursuant to Title 36, including the rights and defenses of a holder in due course, a holder to which a negotiable document of title has been duly negotiated, or a purchaser, respectively if the applicable statutory requirements pursuant to Section 36-3-302, 36-7-501, or 36-9-308 are satisfied. Delivery, possession, and endorsement are not required to obtain or exercise the rights pursuant to this subsection.
(E) Except as otherwise agreed, an obligor under a transferable record has the same rights and defenses as an equivalent obligor under equivalent records or writings pursuant to Title 36.
(F) The person seeking to enforce the transferable record shall provide, upon request, reasonable proof that he is in control of the transferable record. Proof may include access to the authoritative copy of the transferable record and related business records sufficient to review the terms of the transferable record

and to establish the identity of the person having control of the transferable record.

SECTION 26-6-170. Creation and retention of electronic records by government agencies.

Each governmental agency of this State shall determine if, and the extent to which, it will create and retain electronic records and convert written records to electronic records.

SECTION 26-6-180. Government agencies sending and accepting electronic records and signatures; format.

(A) Each governmental agency of this State shall determine if, and the extent to which, it will send and accept electronic records and electronic signatures to and from other persons and otherwise create, generate, communicate, store, process, use, and rely upon electronic records and electronic signatures.
(B) To the extent that a governmental agency uses electronic records and electronic signatures pursuant to subsection (A), the governmental agency, in consultation with the South Carolina State Budget and Control Board, giving due consideration to security, may specify:
(1) the manner and format in which the electronic records must be created, generated, sent, communicated, received, and stored and the systems established for those purposes;
(2) if electronic records must be signed by electronic means, the type of electronic signature required, the manner and format in which the electronic signature must be affixed to the electronic record, and the identity of, or criteria that must be met by, a third party used by a person filing a document to facilitate the process;
(3) control processes and procedures appropriate to ensure adequate preservation, disposition, integrity, security, confidentiality, and auditability of electronic records; and
(4) other attributes required for electronic records which are specified for corresponding nonelectronic records or reasonably necessary under the circumstances.
(C) Except as otherwise provided in Section 26-6-120, this chapter does not require a governmental agency of this State to use or permit the use of electronic records or electronic signatures.

SECTION 26-6-190. Development of standards and procedures; service of process.

(A) The South Carolina State Budget and Control Board shall adopt standards to coordinate, create, implement, and facilitate the use of common approaches and technical infrastructure, as appropriate, to enhance the utilization of electronic records, electronic signatures, and security procedures by and for public entities of the State. Local political subdivisions may consent to be governed by these standards.
(B) The Secretary of State may develop, implement, and facilitate the use of model procedures for the use of electronic records, electronic signatures, and security procedures for all other purposes, including private commercial transactions and contracts. The Secretary of State also may promulgate regulations as to methods, means, and standards for secure electronic transactions including administration by the Secretary of State or the licensing of third parties to serve in that capacity, or both.
(C) In accordance with Sections 26-6-20(18) and 26-6-195, and in reference to all South Carolina laws, rules, and regulations pertaining to service of process where service shall be made on entities described in Rule 4(d)(3) of the South Carolina Rules of Civil Procedure, those entities shall be served under Rule 4(d)(8) of the South Carolina Rules of Civil Procedure by:
(1) registered or certified mail-return receipt requested, addressed to the office of the registered agent;
(2) registered or certified mail-return receipt requested, addressed to the office of the secretary of the corporation at its principal office;
(3) e-mailing the service of process that has been postmarked by a United States Postal Service Electronic Postmark in a manner approved by the South Carolina Supreme Court to an e-mail address registered with the Secretary of State for the corporation; or
(4) e-mailing the service of process that has been postmarked by a United States Postal Service Electronic

Postmark in a manner approved by the South Carolina Supreme Court to an e-mail address registered with the Secretary of State for the agent for service of process for the corporation.

SECTION 26-6-195. Service of process to e-mail address by government agency.

Notwithstanding any other provisions in this chapter, a governmental agency may use, in accordance with policies and procedures developed by the South Carolina Budget and Control Board and as circumstances allow, in order to perfect service of process of any communication, an e-mail address from any vendor, entity, or individual the governmental agency regulates or does business with, or an e-mail address from the agent for service of process of that vendor, entity, or individual. Such communication postmarked by a United States Postal Service Electronic Postmark shall have the same force of law as the United States Post Office certified mail-return receipt requested. The South Carolina Budget and Control Board shall devise policies and procedures for the use of the United States Postal Service Electronic Postmark in respect to state agencies and operations. These policies and procedures, where necessary, must consider the persons or entities which do not have an e-mail address.

SECTION 26-6-210. Applicability of Computer Crime Act.

The Computer Crime Act, as contained in Chapter 16 of Title 16, is expressly made applicable to and incorporated into this chapter.

South Carolina
Enterprise Architecture

Uniform Electronic Transactions Act

SC Standards for Electronic Signatures

February 28, 2007

Table of Contents

1.0 Standards

1.1 Applicability and Scope

Background

The standards promulgated in this document were created in an effort to comply with the purpose and intent of the Uniform Electronic Transactions Act (UETA - S.C. Code Ann. 26-6-10 et seq.). South Carolina Code Section 26-6-190 of UETA, entitled Development of standards and procedures; service of process, states, in part:

> The South Carolina State Budget and Control Board shall adopt standards to coordinate, create, implement, and facilitate the use of common approaches and technical infrastructure, as appropriate, to enhance the utilization of electronic records, electronic signatures, and security procedures by and for public entities of the State. Local political subdivisions may consent to be governed by these standards.

Applicability

As UETA states in S.C. Code Section 26-6-190, the standards set forth in this document are applicable to all State government entities including agencies, boards, commissions, colleges and universities. Local government entities may, at their option, consent to be governed by these standards. Model procedures for the use of electronic records, electronic signatures, and security procedures for private commercial transactions and contracts may be developed, implemented and facilitated by the Secretary of State. Such model procedures addressed in this document may prove applicable for this purpose.

Scope

The UETA does not require State government entities to utilize electronic records or electronic signatures. The extent that State government entities do use such records or signatures, they are subject to these standards (UETA, S.C. Code Section 26-6-180). The purpose of this document is to define the responsibilities and procedures to be used by State government entities when establishing and implementing electronic signatures with regard to the authentication, security, non-repudiation and integrity of such electronic signatures and the electronic records which are to be considered as signed.

Development, Periodic Review and Updating of these Standards

In November 2005, the State Budget and Control Board established a Task Force composed of subject matter experts from a number of state agencies to develop the standards set forth herein. This Task Force submitted its recommendations to the State's Architecture Oversight Committee (AOC) for review, evaluation and adoption. The AOC submitted final recommendations to the State Budget and Control Board, which shall be responsible for maintaining and updating these standards on an ongoing basis. The Task Force has been converted to an UETA Advisory Committee to provide ongoing comments, feedback and advice in this effort.

The Architecture Oversight Committee (AOC), by requiring these standards, does not state or provide the means of funding the assessment, establishment, implementation, or operation of electronic signatures or the electronic transactions which use electronic signatures.

1.2 Applicability to Transactions

The Uniform Electronic Transactions Act (UETA) defines an electronic signature as "*an electronic sound, symbol or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.*" This broad definition becomes problematic when considering the possible types of electronic records as defined by UETA. An electronic record is "*a record created, generated, sent, communicated, received, or stored by electronic means.*" This definition includes not only database records and network-based or web-based data exchanges, but also emails, fax transmissions, voice mails, PDA communications, tape backups and so on. Fax transmissions, voice mails, PDA communications, and tape backups are out of the scope of these standards.

There are four important parts to an electronic signature: 1) an electronic sound, symbol, process, etc. which is unique to the signer; 2) the agreement, either implied or explicit, by both parties to accept an electronic sound, symbol, process, etc. as a valid signature; 3) the intent to sign the record and 4) the action of applying the electronic signature to a specific document or record. These are discussed in greater detail below.

The phrase in UETA "with the intent to sign the record" presupposes that a signature is desired. Fortunately, not all types of electronic records require an electronic signature, nor do they require one to be permanently stored. By their nature, many electronic records do not require a signature, as no contractual, financial or confidential information is being exchanged. Other electronic records, such as a PDF created from a signed paper document, fulfill the requirements of an electronic signature as an intrinsic part of their structure.

The presence of an electronic signature presumes the originality of the record that has been signed. Electronic records must have an authoritative version, which may be treated as an original record, whether or not there are multiple copies of that record. To clarify further, during progressive processing of an electronic record, any information that is added or changed must create a new version of the record, to which the original signature no longer applies. This new record may be stored as (a) separate, duplicate or ancillary record(s). The version to be treated as an original signed version may not change. The new record may in turn be signed, creating a new, separately verifiable electronic signature.

1.3 Standards for Electronic Signatures

All programs implemented by State government entities which utilize electronic signatures shall meet the following conditions. The degree to which these conditions are met will vary by program, as dictated by law or regulation, by risk to the program, or by desire of the participants. Later sections will discuss each of these conditions in greater detail.

> **Use of signature unique to the signer:** The electronic signature must uniquely identify the signer, and must be under reasonable control of the signer. That is, it must be unlikely that any other unauthorized entity provided the signature.
>
> **Agreement by the parties:** A party signs a document in order to convey a mutually understood message to another party, such as authorship, receipt, or approval of the document. In the case of an electronic signature, both the signer and the intended recipient of the signed document must agree, either explicitly or implicitly, that the

electronic sound, symbol, or process will serve as a signature for the electronic document or record.

Intent to sign: The application of the electronic signature to the electronic record must be an intentional act. Intent can be determined by the contents of the document or record and the facts and circumstances surrounding the transaction.

Association of the signature with the signed record: The electronic signature must be physically or logically associated with the electronic record that is signed, and that association must persist for as long as the signature is in effect, which may be the life of the record.

The degree to which each of the above conditions is met is dependent on several factors normally associated with security concerns:

- **Authentication:** the ability to prove that the actual signer is the intended signer,
- **Non-Repudiation:** the inability of the signer to deny the signature, and
- **Integrity:** the assurance that neither the record nor the signature has been altered since the moment of signing.

However, it is important not to confuse the strength of the electronic signature with the strength of the security surrounding a given transaction. For example, an electronic record signed with a digital signature utilizing public key infrastructure (PKI) may be transmitted without authorization over an unsecured network, while a record signed with a weak password may be transmitted in encrypted format over a highly secured line.

Note that this standard does not deny or supersede the implementation standards established by law, regulation, or qualified body for any specific program, such as an IRS / State program or a program governed by HIPAA regulations. Rather, this standard for South Carolina governmental entities is intended to provide a framework for such program specific standards, and to provide governance where no such external standards are in place.

1.4 Use of Signature Unique to the Signer

The electronic sign, symbol, or process serving as the electronic signature must uniquely identify the person, business, agency, or system which is the signer of the electronic record, and be under the reasonable control of that party. The most commonly used form of identification in electronic transactions is the Personal Identification Number (PIN) or password, either assigned arbitrarily to the party by a service provider or self-selected by the party, and used in conjunction with a unique user identification. This PIN or password serves as an electronic signature either by being entered in response to a request to sign a transaction, or by the party's executing an action with intent to sign, while authenticated by the PIN or password. The longer and more complex (use of alpha, numeric, and special characters) the PIN or password is, the less likely that it can be replicated by an unauthorized party. However, the uniqueness of the PIN or password to a given party is still dependent on the security measures taken by the party. The strongest password loses any characteristic of authentication or non-repudiation if it is posted on a sticky note in plain view.

For an individual signer, the strongest form of electronic signature is based on some inherent physical characteristic of the person. A digitized version of a hand-written signature is the simplest example of this class. More sophisticated biometric signatures, such as a digitized fingerprint, retinal scan, or voice print, require more costly technology not readily available at time of this writing to the general public.

For a business, agency, or computer system, the most secure form of electronic signature requires the application of a public/private key pair, often referred to as Public Key Infrastructure (PKI). The business acquires a digital certificate from a Certificate Authority, and installs it on a computer system under secured control. The business or agency utilizes its uniquely assigned private key to sign an electronic record, and the electronic signature generated by this process becomes an intrinsic part of the electronic record. While a digital certificate can be assigned to an individual, this is not general practice, in part because a household computer system is generally shared by multiple parties.

The nature of the sound, symbol, or action to be utilized by a South Carolina agency in a program requiring electronic signatures will depend on several factors. One is the risk to the program of unauthorized or repudiated transactions, and the likelihood of the need to verify the signature in a contested context, such as a court of law. This risk must be balanced against factors of cost and availability of the means of signing for the intended population of signers. A technology which is cost justifiable for a bounded, controlled population such as agency employees or a small, known constituent base, may not be feasible for an unknown and unbounded general public.

It must be noted that while the signing party bears primary responsibility for maintaining control of the means of creating the electronic signature, the recipient of the electronic signature also bears a responsibility to protect the signature on behalf of the signer. For example, an agency that issues PINs or supports PIN self selection must protect those PINs from access by parties who might make unauthorized use of them.

1.5 Agreement by the Parties

For an electronic signature to be valid, both the signing party and the recipient party must agree that the sound, symbol, or process will in fact serve as a signature for the electronic record in question. This agreement may be either formal or informal, and can be determined from the context and surrounding circumstances, including the conduct of the parties. In the business world, electronic commerce is generally established between two parties by means of a Trading Partner Agreement (TPA). The Trading Partner Agreement (TPA) establishes the normal terms and conditions under which the transactions may occur; it sets forth the terms required by the nature of the electronic transaction; and it defines what will constitute a signature if electronic record(s) are to be generated and signed in the course of the transaction. Partners must understand what aspects of an electronic signature are to be implemented, and must understand their responsibility in working with, recognizing and preserving the electronic signature and the associated electronic record(s). In the context of two governmental agencies, whether both agencies are at the state level or at differing federal, state, or local levels, such an agreement is often known as a Memorandum of Understanding or MOU.

For governmental programs involving the general business community or individual constituents, it is not reasonable for an agency to negotiate separate agreements with each party. In this case, the agreement is generally issued unilaterally by the agency through legislation, regulation, or program documentation. Participation in the program by the business or individual party then constitutes acceptance of the agreement and of the program parameters. In all cases, however, there should be advance notice that a sound, symbol, or process generated by the business or individual will be considered to be a valid electronic signature for an electronic record. The simplest form of such notice, in the context of an online transaction, may be wording or a pop-up box on the screen explaining that a subsequent action will be considered to be an act of signing.

1.6 Intent to Sign

There can be no electronic signature without the intention to execute or adopt the sound, symbol or process for purposes of signing the related document or record. There is a sequential

relationship between the agreement by the parties and the act of signing: there is agreement that a certain action will create or serve as an electronic signature, and then that action is intentionally executed. An electronic signature may be created by the signing party or on behalf of a party by an authorized agent, including an electronic agent.

In order to reduce the uncertainty regarding the intent to sign, there should be a prior agreement (or notification) that the execution of the transaction will constitute a signature, followed by the action itself executed with intent to sign. For example, the intent to sign may be demonstrated by a simple mouse click in an online transaction, in response to an on-screen notification that the action will constitute an act of signing. In this case, the signer is generally logged onto an application using credentials such as a user identification and PIN or password, and those credentials may become logically associated with the transaction record to constitute the electronic signature. However, it must be noted that, without the requisite intent to sign, merely executing an online transaction while authenticated by means of certain credentials does not in itself constitute an act of signing, even if those credentials can be associated with the transaction record.

An expression of intent to sign may cover multiple applications of an electronic signature; for example, a system may be programmed to apply a digital signature to all electronic records of a certain type.

1.7 Association of the Signature with the Signed Record

An electronic signature has value only in the context of an electronic record. It may signify that an electronic record is acknowledged or approved, that its contents are agreed to, or that the record is authentic. In the case of the record of a transaction, it may signify that the transaction was properly authorized. The value lies in the ability to verify the signature, and therefore reaffirm its significance to the electronic record, at a later date. For this reason, the electronic signature must be physically or logically associated with the electronic record for the lifetime of the electronic record.

Corollary to this requirement is the assumption that neither the electronic record nor the electronic signature itself is altered during this timeframe. A program utilizing electronic signatures should therefore implement appropriate security measures at both the originator of the signature and the recipient of the signature to prevent unauthorized alteration to either the electronic record or the electronic signature. The nature of these measures may be dictated by external governance, as in the case of an IRS or HIPAA program. If the application of security is at the discretion of the participating South Carolina agency or agencies, then the nature of the security measures should be commensurate to the risk and consequences of unauthorized alteration. A risk assessment should be performed early in the development of the program, in order to determine appropriate security measures to protect the electronic record and electronic signature both during transactions and in subsequent storage.

The simplest of these measures is to ensure that access controls are in place to prevent unauthorized access to modify or delete the electronic record and electronic signature. Stronger measures include the use of unalterable media such as write-once, read many (WORM) disks to store the electronic record and electronic signature. One of the strongest detection measures is the use of digital signatures, where an algorithmic hash of the electronic record is encrypted using the private key of the signer. In this case any alteration to the electronic record by a party not in possession of this private key will invalidate the digital signature, because the digital signature, when decrypted with the signer's public key, will not yield the hash of the altered record.

2.0 Examples

The standard for electronic signatures for South Carolina governmental agencies does not dictate the use of any specific technologies or authorize any specific models for implementation. This is done for two reasons: first, because the array of technologies and implementation models for the use of electronic signatures is extremely large, and would not provide useful guidance for all situations, and secondly so that the technology-neutral standard will not require modification or become invalidated by the invention or adoption of future technology. However, in order to provide some measure of guidance, the following examples of the use of electronic signatures are offered as illustration of the standard.

2.1 Digitized Human Signature

A digitized signature is a graphical image of a handwritten signature. Some applications require an individual to create his or her handwritten signature using a special computer input device, such as a digital pen and pad. The digitized representation of the entered signature may then be compared to a previously-stored copy of a digitized image of the handwritten signature. If special software judges both images comparable, the signature is considered valid. This application of technology shares the same security issues as those using the PIN or password approach, because the digitized signature is another form of shared secret known both to the user and to the system. The digitized signature can be more reliable for authentication than a password or PIN because there is a biometric component to the creation of the image of the handwritten signature. Forging a digitized signature can be more difficult than forging a paper signature since the technology digitally compares the submitted signature image with the known signature image, and is better than the human eye at making such comparisons. The biometric elements of a digitized signature, which help make it unique, are in measuring how each stroke is made (duration, pen pressure, etc.). As with all shared secret techniques, compromise of a digitized signature image or characteristics file could pose a security (impersonation) risk to users.

2.2 Online Tax Filing

The South Carolina Department of Revenue (DOR) offers a web-based application to allow individuals to file their Individual Income Tax returns online. Users are authenticated by means of a pre-assigned PIN which is sent by the DOR to the taxpayer's address of record. At the conclusion of the filing transaction, the user is presented with a "jurat" (Latin for "been sworn") affirming that the information is true and accurate. The user is then prompted to re-enter the PIN as a signature to the jurat and thus the return. By re-entering the PIN, the taxpayer accepts the agreement for that PIN to serve as an electronic signature, and indicates an intent to sign. This use of the PIN therefore constitutes a valid electronic signature.

By contrast, DOR also offers a web-based application to allow businesses to file their Sales and Use Tax returns online. The user must be authenticated by means of a user identification and self-selected PIN prior to utilizing the application. However, the application does not present any jurat to the taxpayer or ask for re-entry of the PIN, nor does it state at any time that any subsequent action will be considered as an act of signing. For this reason, although the online filing is legal and binding, and although proper authentication is required, the transaction is not considered to have been signed.

2.3 Federal / State Tax Filing

When a taxpayer files an electronic income tax return using commercial software such as TurboTax ® or utilizes a paid preparer such as H&R Block, both the federal and state tax returns

are transmitted to the IRS. The IRS, in turn, splits off the state returns and transmits them to the participating states.

The electronic returns are signed by various means, as part of the transaction between the taxpayer and the tax preparer or host of the commercial software, and subsequently the IRS. The DOR considers those returns to be signed, even though the signatures are not verified on receipt by the DOR. This example serves to illustrate the difference between electronic signatures and transactional security. There are a number of security measures in place governing the transactions between the DOR and IRS to retrieve the South Carolina tax returns. However, the authentication of these transactions has nothing to do with the original taxpayers' electronic signatures which are associated with the transmitted electronic records.

3.0 Additional Considerations for Electronic Signatures

3.1 Risk Assessment

Risk Assessment: A risk assessment should be performed to determine the best means of implementing electronic signatures and the level of security for the type of program. This assessment should take into consideration the following issues:

- The nature and value of the data and records in the transactions. Differing types of data and records will have different requirements. Data and records which fall under HIPAA requirements, for example, will have much stricter requirements than some other types of data and records.
- The susceptibility of the transaction's data to fraud. Some data will be of a higher profile, and possibly more susceptible to fraud than other types of data.
- The type of communication for the transactions.
- The security of the systems which host the transaction processes and data.
- The reliability of the systems which host the transaction processes and data.
- The consequences of successful fraud for participants, their organizations and the system(s).
- The role and authority of the user base, especially on those systems where there are multiple levels of authorization on the data.
- The existing technology base and the cost of technology.
- The required level of confidence in establishing the users' identity.
- The required level of communication integrity.
- The required level of record integrity.
- The required level of non-repudiation for records.

Risk Mitigation Plan: After the possible risks have been identified, a risk mitigation plan must be created. This plan will ensure that for all known risks, action will or can be taken to resolve the risk, mitigate the risk, or have a contingency for the risk. Critical risks should be resolved fully prior to proceeding with the implementation. The risk mitigation process should be fully documented.

3.2 Additional Features

There are several additional implementation features of electronic signatures that are not included in the South Carolina standard (as defined in section 1), as they may not apply to all implementations.

These features can fulfill specific business requirements in certain types of business transactions. In some cases, they mimic the process that exists when working with paper documents.

- **Continuity of signature capability:** The ability to ensure that public awareness of the means or technology used to create or apply an electronic signature, such as the identification of the algorithm utilized, does not compromise the ability of the signer to apply additional secure signatures at a later date.
- **Countersignatures:** The capability to prove the order of application of signatures. This is analogous to the normal business practice of countersignatures, where a party signs a document that has already been signed by another party. In an electronic signature, the

issue of record originality must be considered, especially if a copy of the record(s) is made during the process of applying a countersignature.

- **Independent verifiability:** The capability to verify a party's signature (electronic record or digitized signature) without the cooperation of the signer.
- **Interoperability of Electronic Signature Technology:** The assurance that applications, systems or other electronic components used during phases of communication between trading partners and/or between internal components of an entity, are able to read and correctly interpret the transaction information communicated from one to the other.
- **Multiple signatures:** The capability of multiple parties to sign an electronic record, document or transaction. Conceptually, multiple signatures are simply appended to the document or record. Depending upon the implementation, the issue of originality may arise.
- **Data Transportability:** The ability of a signed document to be transported over an insecure network to another system, while maintaining the integrity of the document, including content, signatures, signature attributes, and (if present) document attributes.

4.0 Definitions

AOC: The Architecture Oversight Committee is the governing body of the South Carolina Enterprise Architecture.
Authentication: The use of passwords, tokens (such as smart cards), digital certificates or biometrics to verify that an entity is the one claimed.
Authorization: The process of granting an entity permission to do or have something, or of verifying that permission at time of action.
Ciphertext: The representation of encrypted information. This text may be viewable, but requires decoding. For example, a decryption algorithm is required to convert the ciphertext back into plaintext or its original form.
Credential: A credential is a set of data used for user/system authentication, which is established during a registration process, is stored in an identity management system, and is retrieved for comparison during an authentication process. In some cases, a credential is as simple as a login id and password. Examples of more complex credentials include digital certificates, electronic profiles of a user, a One-Time-Password device, a hardware token, or a biometric device (with the storage of biometric information for a user).
Digital Certificate: A digital certificate is an electronic record issued to a properly authenticated individual or organization by a Certificate Authority (CA). The digital certificate contains a mathematically related pair of encryption keys assigned uniquely to the individual or organization. The "public key" is published by the CA, so that any party may use it to encrypt data intended for the individual or organization. The "private key" must be kept secured by the individual or organization, and is used to encrypt data which can only come from the individual or organization. The digital certificate is installed on a computer system or server controlled by the individual or organization, and is utilized by various communication services, such as web browsers and communication protocols, to perform encryption and decryption services.
Digital Signature: A digital signature is an electronic record created by the mathematical operation of a private encryption key on an electronic record or document. A short record or "digest" is created from the original record or document. The digest is then encrypted with the private key to create the digital signature. The digital signature is generally appended to the document or record for transmission. A digital signature may be verified by the receiving party by decrypting it with the sender's public key, and then comparing the resulting short record with the digest of the transmitted record or document. Digital signatures are considered among the strongest forms of electronic signature for two reasons: 1) they can only be created by an entity's private key, so they are difficult to repudiate, and 2) they are based on a mathematical reduction of the original record or document, so that they cannot be validated if the transmitted record or document is altered in any way.
DOR: Department of Revenue

Electronic Agent: An electronic signature may be created by an electronic agent on behalf of a person. An electronic agent may take the form of software that performs automated processes. An application which accepts electronic signatures from an individual may also need to be configured to authenticate and authorize electronic agents, and to record an electronic signature with the electronic agent as the signer. Note that a computer application may also create an electronic signature on its own behalf, without reference to any specific person.
Electronic Record: A record created, generated, sent, communicated, received or stored by electronic means.
Electronic Signature: Means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.
Embedding: The inclusion or linking of electronic signature elements into the electronic record to which the signature applies.
Encryption: The transformation of confidential plaintext or other information into ciphertext to protect it. An encryption algorithm combines plaintext with other values called keys, or ciphers, so the data becomes unintelligible. Once encrypted, data can be stored or transmitted. Decrypting data reverses the encryption algorithm process and makes the plaintext available for further processing.
HIPAA: Health Insurance Portability and Accountability Act (Pub.L. 104-191, Aug. 21, 1996)
Integrity: The means to ensure that data is complete and unaltered despite aging, transmission, duplication, migration, encryption, decryption or restoration.
IRS: Internal Revenue Service
Jurat: Latin for "been sworn". It pertains to not just affirming the signature is yours but also to swearing the information represented is true and accurate.
Non-repudiation (or non-reputable records): A security feature under which the origin of data cannot be denied, and can be proven to an independent third party.
Password: The confidential authentication information composed of a string of alpha-numeric and / or special characters, whose specific requirements may vary by application, used during an authentication process.
PDA: Personal Digital Assistant (e.g., a Palm Pilot or other handheld electronic equivalent)

PDF: Portable Document Format. A electronic format to convey the image of a document. It is often viewed with Acrobat Reader.
PIN: Personal Identification Number
PKI: Public Key Infrastructure
Record: Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.
UETA: Uniform Electronic Transactions Act. (S.C. Code Ann. Section 26-6-10 et seq.) http://www.scstatehouse.net/code/titl26.htm
WORM: Write Once Read Many. A type of data storage that when once the data is stored, the data cannot be changed.

South Carolina

Electronic Signatures
Analysis and Implementation Guide

March 28, 2007

Proposed by the UETA Task Force,
to the
South Carolina Architecture Oversight Committee

South Carolina

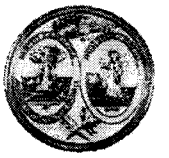
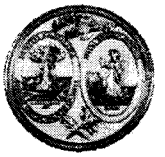


Table of Contents

1. Revision History

First Draft	January 11, 2007	George Felix
Revision	January 31, 2007	Terry Garber
Revision	February 6, 2007	Terry Garber
Revision	February 26, 2007	Terry Garber
Revision	March 6, 2007	Terry Garber



2. Document Overview

This Analysis and Implementation Guide for electronic signatures is intended to assist South Carolina state agencies wishing to implement an electronic commerce program for which signatures are required or desired. It expands upon the foundation of the South Carolina Uniform Electronic Transactions Act provided in the UETA Standards for Electronic Signatures document, hereafter referred to as "the Standards." (UETA SC Standards for Electronic Signatures.doc). For definitions of terms used in this document, please refer to the Standards.

The Standards propose that the validity of an electronic signature is dependent upon four factors:

Use of signature unique to the signer: The electronic signature must uniquely identify the signer, and must be under reasonable control of the signer. That is, it must be unlikely that any other unauthorized entity provided the signature.

Agreement by the parties: A party signs a document in order to convey a mutually understood message to another party, such as authorship, receipt, or approval of the document. In the case of an electronic signature, both the signer and the intended recipient of the signed document must agree that the electronic sound, symbol, or action will be accepted as serving as a signature for the electronic document or record.

Intent to sign: The application of the electronic signature to the electronic record must be a deliberate act. It cannot be implied or inferred.

Association of the signature with the signed record: The electronic signature must be physically or logically associated with the electronic record that is signed, and that association must persist for as long as the signature is in effect, which may be the life of the record.

This document expands on each of these four factors, and explores some of the implementation considerations in each of the four areas.

3. Purpose of a Signature

Signatures are intended to be used to attest:

a. the identity of the person,
b. to the truth and accuracy of information provided, often under penalty of law, and/or
c. to the terms of an agreement (e.g., a contract).

Depending on the circumstances, the signature can be attesting to only one of the above, a combination of any two of the above, or all three.

In the context of an electronic transaction, an electronic signature may be used to attest:

a) the identity of one or more parties to the transaction,
b) to the truth and accuracy of information provided, often under penalty of law,

c) to the terms of an agreement (e.g., a contract) being established by the transaction, and/or
d) to approval to proceed with the transaction (e.g. to file a tax return or charge a credit card).

An electronic signature does not exist in a vacuum; there must be an electronic record which is signed by the electronic signature. This record may exist prior to the transaction, for example, an electronic tax return transmitted to the Department of Revenue by the IRS. It may be created by the transaction, for example, a tax return created by a South Carolina electronic filing application. Or, it may simply be the log or audit record of the transaction itself. In any case, the effectiveness of the signature is dependent on several factors normally associated with security concerns:

- **Authentication:** the ability to prove that the actual signer is the intended signer
- **Non-Repudiation:** the inability of the signer to deny the signature
- **Integrity:** the assurance that neither the record nor the signature has been altered since the moment of signing.

Before using this Analysis and Implementation Guide, the first logical question that agencies must ask is whether their electronic records must be signed at all. As stated in South Carolina's version of the Uniform Electronic Transactions Act and in the South Carolina Standards for Electronic Signatures, state government entities are not required to utilize electronic records or electronic signatures. Three primary determinants of the need for electronic signatures are:

- Is there a legal need for a signature? If the current paper version of the process in question does not require a signature, then the electronic version probably does not require an electronic signature.
- Will there be a need to verify the authentication, non-repudiation, or integrity of an electronic record created by the transaction, independently of the transaction itself, over the life of the electronic record? If not, the agency may need security and authentication processes at the time of the transaction, but may not need the creation of electronic signatures.
- Does the frequency, volume, or complexity of the paper process justify the work to build an electronic process at all, with or without electronic signatures?

To the extent that state government entities do need or choose to utilize electronic records or signatures, they are subject to the standards. Before embarking on new initiatives, agencies should study their requirements and options carefully to ensure that there is a clear business need and that any proposed solution utilizing electronic signatures is appropriate, feasible, and represents a practical trade-off between benefits, costs, and risks. Once a decision has been made to move forward, agencies will find this guide useful and instructive in choosing and implementing the appropriate technology to meet their needs.

4. Risk Assessment Approach

Some or all of the implementation decisions for an agency utilizing electronic signatures may be dictated by legislation, regulation, or the parameters of a national program such as HIPAA. To the extent that the agency is free to design the implementation, key decisions include

- The technology utilized to create the electronic signature
- The method of authenticating the signer and/or the user of the electronic transaction

- The security measures surrounding the execution of the transaction, including the transmission of data, and
- The security measures surrounding the subsequent storage of the signed electronic record.

The recommended approach to making these implementation decisions is a **Risk Assessment** of the entire program and its participants. This assessment should take into consideration issues such as the following:

- The nature and value of the data and records in the transactions. Differing types of data and records will have different requirements. Data and records which fall under HIPAA requirements, for example, will have much stricter requirements than some other types of data and records.
- The susceptibility of the transaction's data to fraud. Some data will be of a higher profile, and possibly more susceptible to fraud than other types of data.
- The consequences of successful fraud for participants, their organizations and the system(s).
- The implications for the program and its participants if the signature is repudiated.
- The type of communication for the transactions.
- The security of the systems which host the transaction processes and data.
- The reliability of the systems which host the transaction processes and data.
- The role and authority of the user base, especially on those systems where there are multiple levels of authorization on the data.
- The existing technology base of all intended participants, and the cost of technology.
- The required level of confidence in establishing the signer's and/or users' identity.
- The implications for the program and its participants if the electronic record is altered; the required level of communication integrity and the required level of record integrity.
- The length of time the electronically-signed records must be retained and made accessible.
- The cost of managing, preserving, and providing access to the signed electronic records during the time period they must be retained.

Risk Management Plan: After the possible risks have been identified, a risk management plan must be created. This plan will examine each dimension of the proposed electronic signature in light of the identified risks. Action may be taken to resolve the risk, mitigate the risk, have a contingency for the risk, or the risk may simply be accepted. Critical risks should be resolved fully prior to proceeding with the implementation. The risk management process should be fully documented.

The remainder of this document discusses each of the four factors of the electronic signature Standards, some of the risks associated with each of the factors, and some of the implementation considerations that may be used to mitigate the associated risk. Examples are then provided of various electronic signature technologies, and of uses of electronic signatures in South Carolina state government.

Please reference the Architecture Oversight Committee's Security Domain, Risk Analysis Discipline.

5. Use of Signature Unique to the Signer

The most fundamental determination regarding this factor of the electronic signature is the nature of the signer. If the signer is a specific human person, then the electronic signature must be reasonably unique to that person. The most unique electronic signatures involve the physical characteristics of the individual. Such "biometric" signatures depend on the digitization of a physical characteristic, such as a finger or thumbprint or retinal scan. The resulting electronic pattern is compared to known patterns to authenticate the signer. A digitized paper signature, although less precise, is still based on physical characteristics of an individual signer.

Alternatively, the signer may in fact be a computer system or server. In the case of a business to government transaction, or agency to agency, the concern may be that the transaction was originated by the proper business or agency, rather than a specific individual. In this case, the appropriate form of signature may utilize a digital certificate issued to the business or agency by a valid certificate authority and installed on a server under control of the business or agency. An application system may generate the proper signature without human intervention.

Other forms of electronic signature may be appropriate to either a human individual or to a business or government entity. A user-id and password, for example, may be thought up by an individual, or they may be randomly generated by a password server application. In either case, in order to be verifiable as an electronic signature, the user-id and password must be registered with, or made known to, the party intended to receive the electronic signature.

Risk assessment concerning this factor of the electronic signature in any program implementation focuses on two areas'

- Failure of authentication – what is the risk to the participants or the program if the signer was not the party that the signer represented himself to be, and
- Repudiation – what is the risk to the participants or the program if the signer denies that he signed the electronic record?

There are two general types of electronic transactions involving electronic signatures. The first is the transmission of a previously created electronic document or record containing an electronic signature. Examples include the retrieval of medical records, or the receipt by the Department of Revenue of a taxpayer return from the IRS. Formats of the electronic signature itself can include the digitized image of a paper signature, the inclusion in the record of a code or PIN assigned to the signer, or a digital signature created from the electronic record by means of a private encryption key, and can represent either an individual or a business or agency. Considerations for this type of electronic transaction include:

- Whether associated risk dictates that every electronic signature must be verified at the time of the transaction, or whether the signature is only verified if the electronic record is contested or repudiated. For example, a digitized paper signature would be impractical if large volumes of electronic transactions required that the signature be verified at the time of the transaction.
- Whether the transmitter of the signed electronic record is a trusted party that has itself verified the electronic signature. For example, the IRS may only transmit valid tax returns to the state.

The second type of electronic transaction is one where the signer is in fact the user of an electronic service such as an online transaction system. In this case, generally some form of authentication of the user takes place when the user logs onto the electronic service or transaction system. The electronic signature is created by some action of the user during the electronic transaction. Considerations for this type of electronic transaction include:

- What is the probability that an unauthorized user can "spoof" the authorized user by logging onto the electronic service or transaction system in place of the authorized user
- What assurance is there that the creator of the electronic signature is the same party who logged onto the electronic service or transaction system? For example, what can happen if the authorized individual human user steps away from the workstation during the transaction. Requiring the user to re-submit the same credentials used to log onto the electronic service or transaction system as the act of signing can reduce the risk that an unauthorized party has taken over the user's access.

Considerations common to both types of electronic transaction involving electronic signatures include:

- What is the level of technology available to the population of signers? For example, if the application is internal to a state agency or group of agencies, it is feasible to issue some form of electronic token to this limited set of signers, or to require the use of digital certificates installed on servers within the agency infrastructure. If this is an application intended for use by the general public, however, then either the issuance of electronic tokens or the requirement for digital certificates is probably neither cost justifiable nor manageable.
- What are reasonable steps that can be taken to increase the probability that the signature is unique to the signer? For example, if cost and availability considerations dictate the use of Personal Identification Numbers (PINs) or passwords, what complexity can be required such as the use of special characters and combinations of alpha and numeric?
- What is the risk that the electronic signature or the electronic record could be accessed during the transaction, providing an unauthorized party with the means to create future invalid electronic signatures? Measures for mitigating this risk include security measures for telecommunications, such as the encryption of the transmitted record or online transaction.

There are several recommended resources that provide guidance in the area of security and authentication of data transmissions and online transactions. This document is not intended to reproduce that guidance, but only to show how these concepts apply to the assurance that the electronic signature was in fact created undeniably by the intended signer. **The reader is referred to the AOC Security Domain for standards in the area of security for South Carolina state agencies.**

6. Agreement by the Parties

The second requirement for use of electronic signatures is an agreement by all parties to transact business electronically. For example, a citizen may not be able to e-mail to a state agency information normally contained in a notarized paper document and assume that the agency will accept the email contents as a signed document.

In the commercial world, businesses enter into peer-to-peer Trading Partner Agreements to spell out the legal, technical, and logistical requirements for the business to conduct electronic commerce. Governmental agencies may execute a similar Memorandum of Understanding to establish agreement. The situation changes, however, in a program offered by a governmental agency to the general public. Clearly it is not feasible to execute separate agreements with a large populace.

In this case, the agreement between the parties may be implicit rather than explicit. The governmental agency offers the electronic program, thereby indicating its willingness to conduct the transaction by electronic means. If the program is voluntary, the citizen indicates his agreement to conduct the transaction electronically by his participation in the program itself. The program may in fact be mandated by law or regulation. In this case the issue of agreement becomes moot.

The risk, in terms of impact on the use of electronic signatures, is that one or both parties will repudiate the transaction. Either the supposed signer will claim that the supposed signing party never agreed that the transaction would represent a signed document or record – for example, that the party never understood that the results of the transaction would be taken as acceptance of contractual conditions – or the recipient will claim that the receiving party never agreed to accept the electronic transaction as a signed document or record. Mitigation of this risk is generally procedural, and may include clear and unequivocal statement in the presentation of an electronic transaction that the completion of the transaction will be considered to be a signed document or record.

7. Intent to Sign

Agreement between the parties refers to a program in general, or a capability to conduct business by electronic means. Intent to sign refers to a specific transaction. There must be clear evidence that the signer intended to complete this particular transaction.

Several forms of electronic signature inherently indicate intent to sign. A paper and ink signature takes a deliberate act to create, so a digitization of that paper signature inherits that intent. A digital signature takes programmatic action to create the encrypted mathematical reduction of the electronic document or record being signed. Electronic transactions that transmit or retrieve documents or records previously signed in either of these manners obtain an intentionally created signature which may be verified if necessary or desired.

Intent to sign becomes more open to question with online transactions. If the user of an online service is properly authenticated at logon to the service, and provides the necessary data for an electronic transaction, it is easy to infer that the user intended to complete the transaction, and to utilize the user's logon credentials as a signature to the transaction. But what if the user enters all of the data, but then shuts down the browser? Did the user intend to complete the transaction, or to cancel it? To assume intent to sign without clear indication of that intent may incur risk that the user may later repudiate the transaction. To mitigate this risk, it is recommended that any online transaction conclude by requiring some affirmative action by the user to indicate clear intent to complete the transaction. This may take the form of a simple "click through," where the user clicks on a button that states "I agree," "I hereby sign," or other appropriate affirmation. However, as noted previously in this document, there may still be a slight risk that the party who

executed the click is not the same party who was authenticated at logon. If this risk is still unacceptable, then stronger risk mitigation is provided by requiring the user to present authentication credentials a second time to serve as an explicit electronic signature. As with Agreement Between the Parties, risk mitigation strategy for Intent to Sign is generally procedural.

8. Association of the Signature with the Signed Record

An electronic signature has no meaning apart from the electronic document or record which it signs. The record may be in the form of business data, such as a tax return or an application for a license; it may be a digitally signed logon request, a request for a medical record, or the retrieved medical record itself. Even though an individual or organization's credentials, such as a user-id and password, a fingerprint, or a physical token, are used for authentication of that individual or organization, unless those credentials are physically or logically associated with a record, with intent to sign the record, no electronic signature has been created. For example, an email that is created and sent is generally accepted as being signed; however, the act of opening and reading an email is generally not considered to have created a signature.

Some electronic signatures, such as the signature on a digitized paper document, cannot be physically separated from the document itself. In most cases, however, the signature is itself a piece of electronic data which can be logically, rather than physically, associated with the record. If a user's authentication credentials are used as an electronic signature on repeated transactions, for example, it would not be sound security practice to store an increasing number of copies of those credentials, increasing the risk of unauthorized use. In this case, some more public form of identification of the party, such as an account number, is used to link the electronic record to the party, with the properly secured credentials available only on an as-needed basis.

Risks associated with this factor of electronic signature implementation include:

- Risk that the signature may be disassociated from the document or record, increasing the possibility of repudiation
- Risk that a signature could be fraudulently associated with an unauthorized document or record
- Risk that a document or record could be modified without authorization after it has been electronically signed.

The form of electronic signature that best addresses these risks is the digital signature. Because a digital signature can only be created using the signer's private encryption key, it is a secure from fraud as the measures that the signer takes to protect that private key. Because the digital signature is created from a mathematical reduction of the electronic record or document, it can be used to detect whether the document has been altered since the digital signature was created. However, it is again noted that digital signature technology, while becoming more commonplace, is still not practical for the general South Carolina public. Moreover, as noted previously, a digital certificate, used to create the digital signature, generally identifies a system or server, rather than an individual. If the identification of an individual person is critical to the validity of an electronic program, then an additional form of authentication and/or electronic signature may be needed to authorize the creation of the digital signature (see Example 5 – SCDPPPS - Offender Supervision - Use of Biometrics).

Whether or not digital signatures are used, reasonable security measures should be taken by all parties to an electronically signed transaction, in order to protect both the electronic signature and

the signed electronic record or document, both during the transaction (in flight) and during their subsequent storage (at rest). This document does not attempt to discuss all of the security measures available; again the reader is referred to the AOC Security Domain standards. However, it must be noted that many electronically signed documents in governmental programs are in fact public records which must be managed in accordance with legally-established record retention schedules and which must be made available on demand, often for extended periods of time. The challenges then becomes ensuring that these records are not altered, forged, or counterfeited and that they are adequately preserved and remain accessible for the full amount of time they must be retained. For additional information on managing, preserving, and providing access to electronic records, refer to the *Electronic Records Management Guidelines* developed by the South Carolina Department of Archives and History (http://www.state.sc.us/scdah/erg/erg.htm), in particular the section on Electronic and Digital Signatures (http://www.state.sc.us/scdah/erg/ermEDS.pdf).

9. Independent Features of an Electronic Signature

An electronic signature is valid if it meets the four characteristics presented in section 2. Beyond these characteristics, however, a specific implementation of electronic signatures may need or wish to provide one or more of the following capabilities. Both business application requirements and risk assessment should be utilized to determine the utility of these features.

- **Continuity of signature capability:** The ability to ensure that public verification or revelation of a signature, encryption method or element of an electronic signature does not compromise the ability of the signer to apply additional secure signatures at a later date.
- **Countersignatures:** The capability to prove the order of application of signatures. This is analogous to the normal business practice of countersignatures, where a party signs a document that has already been signed by another party. In an electronic signature, the issue of record originality must be considered, especially if a copy of the record(s) is made during the process of applying a countersignature.
- **Independent verifiability:** The capability to verify a party's signature (electronic record or digitized signature) without the cooperation of the signer.
- **Interoperability of Electronic Signature Technology:** The assurance that applications, systems or other electronic components used during phases of communication between trading partners and/or between internal components of an entity, are able to read and correctly interpret the transaction information communicated from one to the other.
- **Multiple signatures:** The capability of multiple parties to sign an electronic record, document or transaction. Conceptually, multiple signatures are simply appended to the document or record. Depending upon the implementation, the issue of originality may arise.
- **Data Transportability:** The ability of a signed document to be transported over an insecure network to another system, while maintaining the integrity of the document, including content, signatures, signature attributes, and (if present) document attributes.

10. Examples of Electronic Signatures

Example 1 - Digitized Signature

A digitized signature is a graphical image of a handwritten signature.

Some business processes require an individual to create his or her handwritten signature using a special computer input device, such as a digital pen and pad. The digitized representation of the handwritten signature may then be compared to a previously-stored copy of a digitized image of the handwritten signature. If special software judges both images comparable, the signature is considered valid. This application of technology shares the same security issues as those using the PIN or password approach, because the digitized signature is another form of shared secret known both to the user and to the system. The digitized signature can be more reliable for authentication than a password or PIN because there is a biometric component to the creation of the image of the handwritten signature. Forging a digitized signature can be more difficult than forging a paper signature since the technology digitally compares the submitted signature image with the known signature image, and is better than the human eye at making such comparisons. The biometric elements of a digitized signature, which help make it unique, are in measuring how each stroke is made (duration, pen pressure, etc.). As with all shared secret techniques, compromise of a digitized signature image or characteristics file could pose a security (impersonation) risk to users.

See Example 3 – South Carolina Business One Stop below.

Example 2 – Biometric Signature

Individuals have unique physical characteristics that can be converted into digital form and then interpreted by a computer. Among these are voice patterns (where an individual's spoken words are converted into a special electronic representation), fingerprints, and the blood vessel patterns present on the retina (or rear) of one or both eyes. In this technology, the physical characteristic is measured (by a microphone, optical reader, or some other device), converted into digital form, and then compared with a copy of that characteristic stored in the computer and authenticated beforehand as belonging to a particular person. If the test pattern and the previously stored patterns are sufficiently close (to a degree which is usually selectable by the authenticating application, then the pattern can be verified as the signature of the particular person. Biometric authentication is best suited for access to devices, e.g. to access a computer hard drive or smart card, and less suited as a signature transmitted to a software system over an open network. However, it is an excellent approach when the need to authenticate a signature to a particular individual, as opposed to an organization or computer system, is required.

See Example 5 – SCDPPPS - Use of Biometrics below.

Example 3 – PIN/Password

A password or Personal Identification Number (PIN) is an example of a "shared secret," called "shared" because it is known to both the user and the receiving computer system. The system checks the password or PIN against data in a database to ensure its correctness and thereby

authenticates the user. Passwords and PINs may be entered into a computer system by the user to serve as a signature, in addition to their use to gain access to the system. Unless security is maintained concerning the PIN or password, however, an unauthorized party gaining access to the PIN or password may use it to impersonate the authorized party. Computer applications utilizing PINs and passwords should use security technologies such as encryption both when transmitting and when storing the PIN or password. These measures, however, are meaningless if the user does not also take reasonable precautions.

See Example 1 – EIP Employee Online Benefits Administration and Example 2 – Filing of Sales Tax via Web below.

Example 4 – Digital Signature

To produce a digital signature, a user must obtain or generate by computer two mathematically linked encryption keys – a private signing key that is kept private, and a public validation key that is made available to the public. Neither key can be derived from the other. The use of the public/private key pair is known as Public Key Infrastructure, or PKI. A digital signature must be related to a specific electronic record, such as a document, a data record, or a logon request. To create the digital signature, the computer creates a mathematical digest, or "hash," of the record to be signed. The digest is then encrypted by means of the user's private key. Since the recipient of the digital signature can only encrypt it by means of the user's public key, they recipient can verify that the user created the signature. If the private key has been properly protected from compromise or loss, the signature is unique to the individual or organization that owns it, and the owner cannot repudiate the signature. Moreover, because the digital signature is derived from a mathematical digest of the original electronic record, the record cannot be altered without invalidating the digital signature. The reliability of the digital signature is proportional to the degree of confidence one has in the link between the owner's identity and the digital certificate containing the owner's public and private keys. Note that because PKI relies on computer technology, a digital signature identifies a computer system rather than a particular human individual. For this reason, it is generally used to identify organizations rather than individuals.

See Example 4 – Tax returns between SC Department of Revenue and the IRS below.

Example 5 – Physical Token

A potentially more secure means of entering data to be used both for authentication and as an electronic signature is the use of a physical token, such as a smart card or one-time password device. The signer must be in physical possession of the device, so that it cannot be used by an unauthorized party unless it is lost or shared by the authorized signer. A smart card is a plastic card the size of a credit card containing an embedded integrated circuit or chip that can generate, store, and/or process data. A user inserts the smart card into a card reader attached to a computer. The smart card provides the data for authentication purposes and/or to serve as an electronic signature when the user also enters a PIN, password, or biometric identifier recognized by the card. A one-time password (OTP) device contains an integrated circuit or chip with both a date/time clock and password generation software. The device, which is synchronized with similar software in possession of the intended recipient, continuously generates new passwords at regular time intervals, such as a minute or even a second. When the OTP device is connected to a computer, the generated password may be used either for authentication or to serve as an

electronic signature. Because the password is continuously changing, an unauthorized party cannot reuse a previously used password that the party may be able to acquire.

11. Examples of SC Applications using Electronic Signatures

Example 1 – EIP Employee Online Benefits Administration

Description of Program
The State of South Carolina Employee Insurance Program (EIP) has introduced an internet-based Electronic Benefits System (EBS) to allow eligible employees to access their benefit information and to submit changes electronically to EIP in a total secure environment. Eligible South Carolina Employees will be able to make insurance benefit changes using the online EBS. Upon initial use of the EBS, employees will register online by providing personal information along with their Benefits Identification Number (BIN). This information will be verified against employee data within a master database. Once the employee has successfully registered online, he can view his account or perform direct data entry in the system such as annual / open enrollment or updates such as beneficiary changes or change of address. This program has been developed using industry standard practices and in conformance with regulatory requirements such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Unique Identification of the Party
The employee logs into the system by providing a Benefits Identification Number (BIN) and a password. The BIN has been assigned by the state agency. At the time of registration, employees are required to select a password that must meet certain guidelines that have been established by the Employee Insurance Program and are best practices for security. Such requirements include mixing letters, numbers, and special characters, as well as, a minimum string length.

Agreement by the Parties
The State of South Carolina EIP provides the online EBS for employees to update their insurance benefit options, indicating EIP's agreement to conduct business in this manner. Employees indicate their agreement to make changes to their insurance benefits electronically by registering within and usage of the online EBS. This voluntary act of registering and making online changes constitutes the agreement of parties.

Intent to Sign
Once a state employee has completed changes to the benefits system online, there is a series of explicit actions to accept the changes representing the employee's "intent to sign". There are certain benefit changes that require documents that have a traditional handwritten signature. Such documents are imaged, securely stored and indexed in a relational database.

Association with the Record
The employee's BIN is kept by the Employee Insurance Program along with any associated imaged documents and the subscriber's insurance benefits record.

Security Considerations
In order to insure that a human is making the request within EBS, the subscriber (employee) will be required to repeat a string of characters (i.e., CAPTCHA) displayed within the first screen of the registration routine. Upon successfully entering the string, the subscriber will then be required to enter his/her full name and BIN (Benefits Identification Number). Since the nature of this

transaction involves PHI (protected health information), the system uses a PKI (Public Key Infrastructure) framework in which all transactions are performed over an SSL (Secure Sockets Layer) connection.

References
See **References** on page 18 for the key references used in developing the EIP system architecture and security program.

Example 2 – SCnetFile – Online Individual Income Tax

Description of Program
A South Carolina taxpayer wishes to file and, if necessary, pay Individual Income Tax online. The taxpayer logs onto the system using primary and possibly secondary Social Security Numbers, and a Personal Identification Number (PIN) that was mailed to the taxpayer by the Department of Revenue. The taxpayer then is guided through the submission of tax return data, including W-2 data from employers, and the system computes either the refund due to the taxpayer or else the balance due that the taxpayer must pay the State. If there is a balance due, the taxpayer selects either credit card or direct bank account debit as a payment method. When the taxpayer has entered all data, the taxpayer is shown a page with a "jurat" – a statement that the data that was entered is true and accurate – and is asked to re-enter the PIN to serve as signature.

Unique Identification of the Party
The taxpayer logs onto the system utilizing a PIN that was randomly assigned by the Department of Revenue, and was mailed to the taxpayer's address of record. While the PIN could conceivably be stolen from the mail, the thief would have to know the taxpayer's Social Security Number. There is reasonable assumption that the combination of SSN and PIN would uniquely identify the taxpayer and be known only to the taxpayer.

Agreement by the Parties
The South Carolina Department of Revenue provides the "SCnetFile" online application for filing and paying Individual Income Tax, indicating its agreement to conduct business in this manner. The taxpayer indicates agreement to conduct his personal business of income tax filing electronically by participating in the program. The voluntary act of filing, and if necessary paying, online is all the agreement that is required.

Intent to Sign
The SCnetFile program explicitly instructs the taxpayer to re-enter the PIN to sign the tax return. By re-entering the correct PIN, the taxpayer is again authenticated and performs a deliberate act of signing.

Association with the Record
The electronic Individual Income Tax return is indexed by the Department of Revenue using the taxpayer's primary Social Security Number. This SSN is stored as part of the taxpayer's account record with the Department of Revenue, and all tax returns are associated with the account. The PINs are associated with the SSNs via a separate, and highly secured, file. This file serves to link the PIN to the tax return as needed.

Security Considerations
The taxpayer is authenticated using a PIN that has been previously established. The PIN is transmitted to the taxpayer by US mail in a sealed mailer, and is not provided online or over the telephone, even if requested by the taxpayer. Although fraud is possible, the risk of an unauthorized party filing the return is considered to be only moderate. SSL is used to encrypt all data exchange between the taxpayer and the Department of Revenue. The resulting electronic Individual Income Tax return is stored in a database with controlled, limited access.

NOTE: By contrast, the Department of Revenue e-Sales application for online filing and payment of Sales Tax does not present a jurat or request that any data be entered for the purpose of signing the return. The application is otherwise similar to SCnetFile. While the e-Sales application creates a legally filed tax return, it is not considered by the Department of Revenue to have been signed. There is no legal requirement for a Sales Tax return to be signed.

Example 3 – South Carolina Business One Stop

Description of Program
South Carolina law requires that the Secretary of State receive a signed copy of certain documents. One example is the Articles of Incorporation for a corporation registering to do business in the state. The South Carolina Business One Stop (SCBOS) program is an online application to allow businesses to register electronically with a number of South Carolina agencies, including the Secretary of State. Although registration data is provided in electronic format, SCBOS also supports the ability for the business to upload a scanned pdf copy of the business's Articles of Incorporation.

Unique Identification of the Party
The Articles of Incorporation is a paper document signed in ink by an officer of the corporation and an attorney. These signatures, even when digitized, are provably unique to the signer as described above.

Agreement by the Parties
By providing the capability to upload a digitized copy of the Articles of Incorporation through the SCBOS program, the Office of the Secretary of State indicates its agreement to accept this as a signed document. By completing the action of uploading the digitized Articles, the business indicates its agreement to provide this electronic signature and to conduct this electronic transaction.

Intent to Sign
The business is asked to demonstrate intent to sign twice – first, by applying an ink signature in the appropriate place on the paper Articles of Incorporation, and secondly by uploading the signed document in pdf format. The SCBOS program asks the user to provide this signature, which is an intentional act.

Association with the Record
Because the ink signature is an integral part of the paper Articles of Incorporation, the digitized signature is an integral part of the digitized Articles of Incorporation in pdf format. As long as the pdf file is preserved intact, the signature will remain a part of the record.

Security Considerations
The signature on the pdf Articles of Incorporation is assumed to be valid with low risk, the same as if the paper version were brought to the Secretary of State. Self-selected user-id and password are used to register and authenticate the business user. Secure Socket Layer (SSL) encryption is used to secure SCBOS data exchange, to protect sensitive information such as Social Security Numbers during the transaction.

Example 4 – Tax returns between SC Department of Revenue and the IRS

Description of Program
An individual files an electronic Individual Income Tax return using a preparer such as H&R Block, or a third party software such as TurboTax™. The individual is asked to enter a self-selected PIN to serve as signature. Both federal and state returns are transmitted to the IRS. IRS splits out and batches the state returns and makes them available to the state for download. IRS is in the process of implementing a process where the state digitally signs its logon request to the IRS using a previously registered digital certificate.

Unique Identification of the Party
The taxpayer's PIN is self-selected, so it can be assumed to be under the unique control of the taxpayer. However, duplication across millions of taxpayers is possible, so the PIN is used in combination with the filer's Social Security Number for taxpayer identification. The state must obtain a unique digital certificate from a commercial certificate authority. The private key used to encrypt the state's logon uniquely identifies the trusted computer system used to communicate with the IRS.

Agreement by the Parties
The IRS sanctions electronic filing of Individual Income Tax by use of approved third parties. Its acceptance of electronically filed returns from these parties indicates IRS agreement to transact business in this manner. Electronic filing is voluntary, so the taxpayer's use of an electronic filing program, either through a paid preparer or through third party software, indicates the taxpayer's agreement to transact business electronically.

Intent to Sign
All electronic filing software approved by the IRS explicitly asks the taxpayer to enter the self-selected PIN to sign the return. The use of the PIN is therefore a deliberate act of signing. The state's communications gateway with IRS creates a digital signature from the electronic record created as its logon request. Although this is an automated function, the fact that this program was created and implemented by the state makes this an intentional act of signing.

Association with the Record
The taxpayer PIN is retained by IRS in association with the taxpayer's return. The digital signature of the state's logon request to IRS is created from the logon request record itself, and is logically associated in that the logon record cannot be altered without invalidating the electronic signature.

Security Considerations
Although there is known to be some amount of fraud associated with electronic tax filing, it generally does not involve misrepresentation of the identity of the filer. For that reason, the self-

selected PIN is accepted by IRS as electronic signature. The state assumes that IRS has validated this signature, and does not re-authenticate the signature. The transmission of batches of tax returns from the IRS to the state, however, contains highly sensitive information. For that reason, the IRS requires the digitally signed logon to ensure that the state's tax returns are transmitted only to the state. The data is encrypted during transmission. The state then stores these electronic returns using controlled limited access storage.

Example 5 – SCDPPPS - Offender Supervision - Use of Biometrics

Description of Program
The South Carolina Department of Probation, Pardon and Parole Service (SCDPPPS) has a future example of the use of biometrics. Future Department offender supervision business processes conducted by agents will be enhanced through the use of biometrics. This will afford real-time offender data capture and information storage through the agent's issued tablet PCs. Agents will be able to effect data collection, signature, and immediate information storage on the tablet for subsequent synchronization with the Department's main database.

Unique Identification of the Party
Currently, agents are required to register in person, and only with authorization from their manager to obtain their tablet PC. The future registration process will involve setting up agents' logins and passwords and recording their fingerprints for biometric identification. This information will be recorded as a Credential in both the Department's main information system as well as on agent PCs.

Additionally, supervised offenders are also required to register a fingerprint through use of a biometric identification device.

Agreement by the Parties
As a matter of Department business practice and processes inherent with offender supervision, agents agree to the use of biometrics to register their digital signatures.

Intent to Sign
When an agent is required to certify who created a business transaction, the ultimate goal will be to use the registered fingerprint, plus an issued PIN, as the certification mechanism.

Longer term, the use of kiosks to conduct some business transactions will also be facilitated by the same process.

Association with the Record
This two-part authentication activates a standard digital certificate and will be used to apply the digital signature from the agent's machine to the offender case supervision business processes and is retained with the record(s).

Security Considerations
The agent is authenticated by both the fingerprint and their login user id and password. The password requires a mix of numbers, letters, and special characters to make it more difficult to

guess. The use of the finger print is more secure for authentication due to the high risk of this application. The use of the digital signature securely identifies the source of the transaction and allows the recipient to determine if the document has been altered.

12. References

South Carolina UETA act (In S.C. Code Ann. 26-6-10 et seq.)
http://www.scstatehouse.net/code/titl26.htm

The State of Texas: Guidelines for the Management of Electronic Transactions and Signed Records Prepared by the UETA Task Force of the Department of Information Resources and the Texas State Library and Archives Commission
http://www.dir.state.tx.us/standards/UETA_Guideline.htm

An online dictionary and search engine for computer and Internet technology definitions.
http://www.webopedia.com/

Risk Assessment
United States General Accounting Office Information Security Risk Assessment Practices of Leading Organizations: http://www.gao.gov/special.pubs/ai00033.pdf

A copy of the UETA document with embedded comments:
http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm

National Conference of Commissioners on Uniform State Laws
Home Page
http://www.nccusl.org/Update/
Summary of UETA
http://www.nccusl.org/Update/uniformact_summaries/uniformacts-s-ueta.asp
Why States should adopt UETA
http://www.nccusl.org/Update/uniformact_why/uniformacts-why-ueta.asp
A few facts about UETA
http://www.nccusl.org/Update/uniformact_factsheets/uniformacts-fs-ueta.asp

United States Postal Service – Electronic Postmark (EPM) and its use of auditable time stamps, digital signatures and hash codes.
http://www.usps.com/electronicpostmark/welcome.htm

South Carolina Department of Archives and History
Electronic Records Management Guidelines http://www.state.sc.us/scdah/erg/erg.htm
Electronic and Digital Signatures http://www.state.sc.us/scdah/erg/ermEDS.pdf

Security Links

Wireless Search - http://www.shmoo.com/gawd/

Cisco Security Page (good white papers on "Best Practices") -
http://www.cisco.com/go/security

CERT Web Page (Computer Emergency Response Team) - http://www.cert.org

Good Hacking Sites (shows exploits that you may want to be aware of):
http://packetstormsecurity.com/
http://www.securityfocus.com/

More Security Best Practices References:
• An Introduction to Computer Security: The NIST Handbook
- http://csrc.nist.gov/publications/nistpubs/800-12/
• Federal Agency Security Practices
- http://csrc.nist.gov/fasp/
• CERT Guide to System and Network Security Practices
- http://www.cert.org/security-improvement/#practices
• Security Self-Assessment Guide for IT Systems: NIST Special Publication 800-26
- http://csrc.nist.gov/publications/nistpubs/index.html

Key references used in developing the EIP system architecture and security program

Centers for Medicare and Medicaid Services (CMS). This government website provides the Health Insurance Portability and Accountability Act of 1996 (HIPAA) rules and regulations such as the Security Standard and the Transactions and Code Sets Standards. http://www.cms.hhs.gov/home/regsguidance.asp
Directly to the document:
http://www.cms.hhs.gov/TransactionCodeSetsStands/Downloads/txfinal.pdf

National Institute of Standards and Technology's (NIST) Computer Security Resource Center (CSRC). The special publications 800 series presents the results of NIST studies, investigations, and research on information technology security issues. http://csrc.nist.gov/publications/

The Workgroup for Electronic Data Interchange (WEDI). Healthcare industry group focusing on development and implementation of healthcare industry standards, policies and regulations; http://wedi.org/

Health Level Seven (HL7) is an American National Standards Institute (ANSI) accredited Standards Developing Organization (SDO) operating in the healthcare arena. Health Level Seven's domain is clinical and administrative data. http://hl7.org/

The American National Standards Institute (ANSI) coordinates the development and use of voluntary consensus standards in the United States and represents the U.S. stakeholders in standardization forums around the globe. The ANSI X12 standards has been adopted for use in HIPAA financial transactions for health care (ex. 834 Benefit Enrollment and Maintenance and 837 Claims). http://www.ansi.org

Office of State Fire Marshal Fire Sprinkler System Review Process

Current Review Process

Construction document package received by receptionist

Receptionist opens package to retrieve the documents, stamps in the documentswith the date and time received

Receptionist delivers documents to administrative assistant for engineering section

New project?

No → Administrative assistant pulls existing file, logs the new data on the project into the database under the existing database number

Administrative assistant delivers project file to assigned reviewer

Yes → Administrative assistant assigns it a project number and logs it into the database

Project is assigned to next engineer on rotation and delivered by administrative assistant

Reviewer places the documents in their queue of projects awaiting review. Order based on date of receipt

Reviewer reviews the documents in order of date received and adds information to the data sheet

Documents have been prepared by properly licensed individuals and/or companies?

No → Return letter issued citing reason and state statute → Administrative assistant updates database information based on returned file information and datasheet

Yes → Documents are sufficiently complete to conduct a review?

No → If not complete, reviewer issues a return letter stating the information needed to conduct a review → Administrative assistant updates database information based on returned file information and datasheet

Yes → Reviewer determines the extent to which a review must be conducted, full versus partial. Reviewer then reviews the documents to determine if the documents meet all of the applicable fire & life safety codes based on the extent of review chosen

Compliance issues?

No → If no compliance problems are noted, an approval or acceptance letter is written and submitted to the administrative assistant for typing along with placement in the project file → Administrative assistant updates database information based on returned file information and datasheet → Administrative assistant types letter for review and signature → If no edits, signed letter is copied by adminiatrative assistant for all appropriate parties and mailed → Administrative assistant files plans and retains file and plans for a minimum of three years

Yes → Plans substantially compliant?

No → If not substantially compliant, a Not Approved letter typing request is submitted to the administrative assistant along with the project file → If the project is resubmitted, the reviewer compares the resubmitted documents to the unresolved items listed on the last review letter to determine if they have been addressed

Yes → If substantially compliant with only minor compliance issues, a Conditional Approval or Conditional Acceptance letter typing request is submitted to the administrative assistant along with the project file → Administrative assistant updates database information based on returned file information and datasheet → Administrative assistant types letter for review and signature. If no edits, signed letter is copied by administrative assistant for all appropriate parties and mailed → Administrative assistant files plans and retains file and plans for a minimum of three years

Task	Current Plan Review Process	Estimated Time Spent on Process	Value Added	Non Value
Construction documents package received by receptionist (by mail, courier, Fed-Ex, UPS, etc.)		.5 day – 1 week		
Delay in stamping in the documents and delivering the documents to the engineering adminstrative assistant		.5 day - 2 days		
Receptionist opens package to retrieve documents		5 minutes		
Receptionist stamps each document with current date and time using UL Listed time recorder machine		5 minutes		
Receptionist delivers documents to administrative assistant for engineering section		2 minutes		
Delay in engineering administrative assistant logging the plans in and assigning them to the project engineer		1 - 2 days		
Administrative assistant determines if documents are new or existing project		10 minutes		
If new project, administrative assistant assigns it a project number on a sequential basis and with an appropriate project type letter tag (S or U for sprinkler type plans depending on the scope of work on the sprinkler system)		5 minutes		
If new project, administrative assistant assigns it to the next reviewer on a rotating basis		3 minutes		
If new project, administrative assistant logs certain data on project in database under the new project number		3 minutes		
If new project, administrative assistant creates a file for the newly received documents and attaches a printout of the database information		3 minutes		
If existing project, administrative assistant pulls existing file		3 minutes		
If existing project, administrative assistant logs the new data in the project into the database under the existing project number		3 minutes		
Administrative assistant delivers project file to assigned reviewer		1 minute		
Reviewer places the documents in their queue of projects awaiting review (order based on date of receipt)		1 minute		
Delay in review process due to order in which the project was received		1 - 3 weeks		
Reviewer reviews the documents in order of date received and adds information to the data sheet		5 minutes		
Reviewer determines if documents have been prepared and authorized (signed, sealed, etc.) by properly licensed individuals and/or companies		5 minutes		
Reviewer determines if documents are sufficiently complete to conduct a review		5 minutes		
If not duly authorized or sufficiently complete, reviewer issues a RETURN letter stating the information/documentation/authorization needed to conduct a review		10 minutes		
If duly authorized and sufficiently complete, reviewer determines extent of review to be conducted. Documents submitted without a Certificate of Compliance, when not required to, have one must receive a FULL REVIEW. Documents submitted with a Certificate of Compliance may receive a partial COC Review.		5 minutes		
Reviewer then reviews the documents to determine if the documents meet applicable adopted fire and life safety codes based on the extent of review chosen		4 hours		
If no compliance problems are noted, an Approval or Acceptance letter typing request is submitted to the administrative assistant along with the project file		5 minutes		
If substantially compliant with only minor compliance problems, a Conditional Approval or Conditional Acceptance letter typing request is submitted to the administrative assistant along with the project file		10 minutes		
If not substantially compliant, a Not Approved letter typing request is submitted to the administrative assistant along with the project file		15 minutes		
If the project is a resubmittal, the reviewer compares the resubmitted documents to the unresolved items listed on the last review letter and determines if the items have been resolved		15 minutes		
If the items have been resolved, an Approval or Acceptance letter typing request is submitted to the administrative assistant along with the project file		5 minutes		
If the items have not all been resolved, however corrected documents are substantially compliant with only minor compliance problems, a Conditional Approval or Conditional Acceptance letter typing request is submitted to the administrative assistant along with the project file		10 minutes		
If the items have not all been resolved, and the corrected documents are not substantially compliant, a Not Approved letter typing request is submitted to the administrative assistant along with the project file		15 minutes		
Delay in engineering administrative assistant typing the letter for the project engineer and delivering the project file and letter back to the reviewing engineer		2 days		
Administrative assistant updates database information based on returned file information and data sheet		5 minutes		
Administrative assistant assigns a storage box number to documents, drawings and/or specifications, that are too big to be stored in the file folder and then records the box number in the data base		2 minutes		
The administrative assistant places the subject large and/or thick documents in a storage box		2 minutes		
The administrative assistant files the storage box with the others in a specially assigned storage area		2 minutes		
Administrative assistant types up letter for review		2 minutes		
Administrative assistant returns file to reviewer with typed letter		10 minutes		
Reviewer reviews and if needed edits typed letter		5 minutes		
If no edits to letter, reviewer signs letter		1 minute		
If edits to letter, reviewer returns letter to administrative assistant for correction and repeats the process until he signs the letter		1 minute		
Delay in making corrections to letter by engineering administrative assistant		1 day		
Delay in reviewing engineer delivering letter back to engineering administrative assistant		1 day		
Signed letter is delivered to administrative assistant with file		1 minute		
Administrative assistant makes copies of the signed letter for the file, the designer, each part listed as a CC on the letter		20 minutes		
Administrative assistant prints addressed envelopes for each letter to be mailed out		2 minutes		
Administrative assistant mails original letter to designer and a copy to each, if any, CC listed on the letter		1 minute		
Administrative assistant places a copy of the letter in the project file		10 minutes		
Administrative assistant places the project file in the queue of projects awaiting filing/refilling		1 minute		
Administrative assistant retains the project file and associated documents for a minimum of 3 years from date of first receipt then purges them from file.				
		29 days 4 hours		

Office of State Fire Marshal Fire Sprinkler System Review Process

Electronic Review Process

Construction document package received by the computer mail server

New project?

No

Administrative assistant pulls up existing file information, logs the new data on the project into the database under the existing database number

Yes

Administrative assistant assigns it a project number and logs it into the database

Project is assigned to next engineer on rotation and delivered by administrative assistant to reviewing engineer

Administrative assistant delivers project file to assigned reviewer

Reviewer places the documents in their queue of projects awaiting review. Order based on date of receipt

Reviewer reviews the documents in order of date received and adds information to the data sheet

Documents have been prepared by properly licensed individuals and/or companies?

No

Return letter issued citing reason and state statute

Administrative assistant updates database information based on returned file information and datasheet

Yes

Documents are sufficiently complete to conduct a review?

No

If not complete, reviewer issues a return letter stating the information needed to conduct a review

Administrative assistant updates database information based on returned file information and datasheet

Yes

Reviewer determines the extent to which a review must be conducted, full versus partial. Reviewer then reviews the documents to determine if the documents meet all of the applicable fire & life safety codes based on the extent of review chosen

Compliance issues?

Yes

Plans substantially compliant?

No

If not substantially compliant, a Not Approved letter typing request is submitted to the administrative assistant along with the project file and the letter is placed in the submitters private electronic mailbox for retrieval.

If the project is resubmitted, the reviewer compares the resubmitted documents to the unresolved items listed on the last review letter to determine if they have been addressed

Yes

If substantially compliant with only minor compliance issues, a Conditional Approval or Conditional Acceptance letter typing request is submitted to the administrative assistant along with the project file

Administrative assistant updates database information based on returned file information and datasheet

Administrative assistant types letter for review and signature. If no edits, signed letter is copied by administrative assistant for all appropriate parties and mailed

No

If no compliance problems are noted, an approval or acceptance letter is written by the reviewing engineer and submitted to the administrative assistant review along with placement in the project file and the customers private mail box

Administrative assistant updates database information based on returned file information and datasheet

Administrative assistant files the electronic plans in the proper electronic project file for life.

Task	**Proposed Electronic Plan Submission, Review and Data Storage System**	Estimated Time on Process	Value Added	Non Value
Construction documents package received by electronic transmission				
Delay in engineering administrative assistant logging the plans in and assigning them to the project engineer		1 - 2 days		
Administrative assistant determines if documents are new or existing project		10 minutes		
If new project, administrative assistant assigns it a project number on a sequential basis and with an appropriate project type letter tag (S or U for sprinkler type plans depending on the scope of work on the sprinkler system)		5 minutes		
If new project, administrative assistant assigns it to the next reviewer on a rotating basis		3 minutes		
If new project, administrative assistant logs certain data on project in database under the new project number		3 minutes		
If new project, administrative assistant creates a file for the newly received documents and attaches a printout of the database information		3 minutes		
If existing project, administrative assistant pulls existing file		3 minutes		
If existing project, administrative assistant logs the new data in the project into the database under the existing project number		3 minutes		
Delay in administrative assistant delivering project file to assigned engineer		4 hours		
Administrative assistant delivers project file to assigned reviewer		1 minute		
Reviewer places the documents in their queue of projects awaiting review (order based on date of receipt)		1 minute		
Delay in review process due to order in which the project was received		1 - 3 weeks		
Reviewer reviews the documents in order of date received and adds information to the data sheet		5 minutes		
Reviewer determines if documents have been prepared and authorized (signed, sealed, etc.) by properly licensed individuals and/or companies		5 minutes		
Reviewer determines if all required documents are submitted and sufficiently complete to conduct a review		5 minutes		
If not duly authorized or sufficiently complete, reviewer issues a RETURN letter stating the information/documentation/authorization needed to conduct a review		10 minutes		
If duly authorized and sufficiently complete, reviewer determines extent of review to be conducted. Documents submitted without a Certificate of Compliance, when not required to, have one must receive a FULL REVIEW. Documents submitted with a Certificate of Compliance may receive a PARTIAL COC REVIEW.		5 minutes		
Reviewer then reviews the documents to determine if the documents meet applicable adopted fire and life safety codes based on the extent of review		4 hours		
If no compliance problems are noted, an APPROVAL or ACCEPTANCE letter is submitted to the administrative assistant along with the project file		5 minutes		
If substantially compliant with only minor compliance problems, a CONDITIONAL APPROVAL or CONDITIONAL ACCECPTANCE letter is submitted to the administrative assistant along with the project file		10 minutes		
If not substantially compliant, a NOT APPROVED letter is submitted to the administrative assistant along with the project file		15 minutes		
If the project is a resubmittal, the reviewer compares the resubmitted documents to the unresolved items listed on the last review letter and determines if the items have been resolved		15 minutes		
If the items have been resolved, a signed APPROVAL or ACCEPTANCE letter is submitted to the engineering administrative assistant along with the project file		5 minutes		
If the items have not all been resolved, however corrected documents are substantially compliant with only minor compliance problems, a signed CONDITIONAL APPROVAL or CONDITIONAL ACCEPTANCE letter is submitted to the engineering administrative assistant along with the project file		10 minutes		
If the items have not all been resolved, and the corrected documents are not substantially compliant, a signed NOT APPROVED letter is submitted to the engineering administrative assistant along with the project file		15 minutes		
Administrative assistant updates database information based on returned file information and data sheet		5 minutes		
Administrative assistant makes copies of the signed letter for each party listed as a CC on the letter		20 minutes		
Administrative assistant prints addressed envelopes for each letter to be mailed out		2 minutes		
Administrative assistant places original PDF letter to designer in their secure mail box for retreival		2 minutes		
Administrative assistant places a copy of the letter in the project file		10 minutes		
Administrative assistant retains the project file and associated documents for life				
		18 days 2 hrs. 54 minutes		

Electronic Sprinkler Plans Submission Survey

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

	Response Count
	47
answered question	**47**
skipped question	**0**

2. Does it allow you to save the design drawings as a .dwg format?

	Response Percent	Response Count
A. Yes	**93.6%**	44
B. No	6.4%	3
answered question		**47**
skipped question		**0**

3. Does it allow you to save the design drawings as a .dwf format?

	Response Percent	Response Count
A. Yes	**79.5%**	35
B. No	20.5%	9
answered question		**44**
skipped question		**3**

4. What is the largest CAD file size you have ever produced (in megabytes)?

	Response Percent	Response Count
A. 5	7.0%	3
B. 10	16.3%	7
C. 15	9.3%	4
D. 20	**32.6%**	14
E. 30	18.6%	8
Other (please specify)	11.6%	5
answered question		**43**
skipped question		**4**

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

	Response Percent	Response Count
A. Yes	**89.1%**	41
B. No	10.9%	5
answered question		**46**
skipped question		**1**

6. If so, what software?

	Response Count
	47
answered question	**47**
skipped question	**0**

7. Do you have the ability to transmit and receive electronic files?

	Response Percent	Response Count
A. Yes	**97.9%**	46
B. No	2.1%	1
answered question		**47**
skipped question		**0**

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

	Response Percent	Response Count
A. Yes	**84.4%**	38
B. No	15.6%	7
answered question		**45**
skipped question		**2**

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

	Response Percent	Response Count
A. Yes	**75.0%**	33
B. No	25.0%	11
answered question		**44**
skipped question		**3**

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?			
		Response Percent	Response Count
A. Yes		91.3%	42
B. No		8.7%	4
	answered question		46
	skipped question		1

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?		
		Response Count
		47
	answered question	47
	skipped question	0

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 47 of 47 respondents

Response Type: Normal Response
Collector: Survey (Web Link)
Custom Value: *empty*
IP Address: 216.248.156.194
Response Started: Tue, 8/12/08 5:32:22 PM
Response Modified: Tue, 8/12/08 5:35:59 PM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

AutoCAD version 2009

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

E. 30

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

WINZIP

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

B. No

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

not at this time.

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 46 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 12.107.235.89
Response Started: Fri, 8/1/08 4:33:53 PM	**Response Modified:** Fri, 8/1/08 4:37:13 PM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

Microstation

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

D. 20

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

WinZip

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

What is the anticipated review of the sprinkler shop drawings with the sprinkler designer and the consulting engineer? Are the drawings send the engineer before transmitting to the local or state agency. I'm not aware of other jurisdications who review electronic sprinkler drawings/design. This is a great idea and will be benefical to the industry.

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 45 of 47 respondents

Response Type: Normal Response
Collector: Survey (Web Link)
Custom Value: *empty*
IP Address: 70.155.167.76
Response Started: Mon, 7/28/08 3:58:56 PM
Response Modified: Mon, 7/28/08 4:08:11 PM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?
HYDRACAD

2. Does it allow you to save the design drawings as a .dwg format?
A. Yes

3. Does it allow you to save the design drawings as a .dwf format?
A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?
E. 30

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?
A. Yes

6. If so, what software?
WINZIP

7. Do you have the ability to transmit and receive electronic files?
A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?
A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?
A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

TO REDUCE THE SIZE OF DWGS CONVERT THEM TO PDF IT WILL MORE THAN CUT THE SIZE IN HALF

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 44 of 47 respondents

Response Type: Normal Response
Collector: Survey (Web Link)
Custom Value: *empty*
IP Address: 64.128.213.93
Response Started: Thu, 7/24/08 10:28:12 AM
Response Modified: Thu, 7/24/08 10:35:42 AM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

Hydracad

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

B. No

4. What is the largest CAD file size you have ever produced (in megabytes)?

Other (please specify) - 45m

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

windzip

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

We think this would be wonderful and save alot of time. Lori Performance Fire Protection, LLC

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 43 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 66.191.213.225
Response Started: Wed, 7/23/08 9:42:00 AM	**Response Modified:** Wed, 7/23/08 9:43:41 AM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

autocadd 2007

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

B. 10

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

Zip

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

B. No

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

B. No

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

no

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 42 of 47 respondents

Response Type: Normal Response
Collector: Survey (Web Link)
Custom Value: *empty*
IP Address: 66.35.169.114
Response Started: Tue, 7/22/08 7:30:41 AM
Response Modified: Tue, 7/22/08 7:33:12 AM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?
hydracad

2. Does it allow you to save the design drawings as a .dwg format?
A. Yes

3. Does it allow you to save the design drawings as a .dwf format?
A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?
E. 30

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?
A. Yes

6. If so, what software?
win zip

7. Do you have the ability to transmit and receive electronic files?
A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?
A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?
A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

I think it would help speed the process greatly. I'm glad you are considering doing this.

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 41 of 47 respondents

Response Type: Normal Response
Collector: Survey (Web Link)
Custom Value: *empty*
IP Address: 209.208.18.186
Response Started: Tue, 7/22/08 6:23:19 AM
Response Modified: Tue, 7/22/08 6:27:37 AM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?
HydraCad

2. Does it allow you to save the design drawings as a .dwg format?
A. Yes

3. Does it allow you to save the design drawings as a .dwf format?
A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?
D. 20

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?
A. Yes

6. If so, what software?
winzip

7. Do you have the ability to transmit and receive electronic files?
A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?
A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?
A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

The City of Winston-Salem, NC does electronic plan review and the City of Charlotte does their own version of electronic plan review as well. In this day there is very little reason why not to submit plans electronically. Our company would prefer to do electronic plan review.

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 40 of 47 respondents

Response Type: Normal Response
Collector: Survey (Web Link)
Custom Value: *empty*
IP Address: 71.12.70.75
Response Started: Mon, 7/21/08 12:25:56 PM
Response Modified: Mon, 7/21/08 12:30:04 PM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?
AutoCad

2. Does it allow you to save the design drawings as a .dwg format?
A. Yes

3. Does it allow you to save the design drawings as a .dwf format?
A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?
E. 30

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?
A. Yes

6. If so, what software?
ZIP

7. Do you have the ability to transmit and receive electronic files?
A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?
A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?
A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

We are a Civil consulting firm and deal strictly with u/g FP protection submittals to your office. It would be a great convenience to make submittals electronically.

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 39 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 65.196.101.212
Response Started: Mon, 7/21/08 9:57:47 AM	**Response Modified:** Mon, 7/21/08 10:00:17 AM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

AUTOCAD 2008

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

D. 20

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

winzip or winrar

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

I think it is great and would save time. You might want to think about instead of sending .dwg files, the newer versions of autocad allow you to save as .pdf files and those would be easier to send and read.

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 38 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 70.43.117.34
Response Started: Mon, 7/21/08 9:45:10 AM	**Response Modified:** Mon, 7/21/08 9:50:00 AM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

AutoDesk AutoCadd V.8

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

B. 10

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

winzip

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

I have never dealt with electronic seals or signatures. I'm pretty sure we can do it; it's just a matter of learning how. Also, as of right now, you require a handwritten signature on the submitted drawings, will this be replaced by the electronic signature?

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 37 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 167.7.81.64
Response Started: Mon, 7/21/08 9:32:20 AM	**Response Modified:** Mon, 7/21/08 9:44:08 AM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

AutoCAD 2007

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

No Response

4. What is the largest CAD file size you have ever produced (in megabytes)?

Other (please specify) - over 4 megs is tough to open

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

winzip

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

We recommend transmission in PDF format, because lineweights, fonts, drawing content is not compromised. With Adobe Pro, you may be able to red line the PDF drawing - this is worth investigating.

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 36 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 66.83.151.218
Response Started: Mon, 7/21/08 7:49:24 AM	**Response Modified:** Mon, 7/21/08 7:51:42 AM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

AutoCAD 2009

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

C. 15

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

Winzip

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

B. No

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

Perhaps I am old fashioned, but prefer the submittal of signed and sealed drawings by paper copy. We have had some difficulty in the past: when other people have printed our electronic drawings, they do not look exactly like the ones we print.

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 35 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 76.26.207.223
Response Started: Sun, 7/20/08 9:15:45 PM	**Response Modified:** Sun, 7/20/08 9:18:14 PM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

Revit

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

Other (please specify) - 100 mb+

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

Adobe acrobat

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

Consider using Adobe PDF with electronic seals and signatures.

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 34 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 169.130.158.66
Response Started: Sat, 7/19/08 8:11:17 PM	**Response Modified:** Sat, 7/19/08 8:16:06 PM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

HydraCAD, AutoCAD 2007/2009

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

D. 20

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

AutoCAD; Windows

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

All of the new CAD software can print the drawings in PDF format also.

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 33 of 47 respondents

Response Type: Normal Response
Collector: Survey (Web Link)
Custom Value: *empty*
IP Address: 64.16.230.151
Response Started: Fri, 7/18/08 4:48:39 PM
Response Modified: Fri, 7/18/08 5:12:45 PM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

AutoCAD

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

Other (please specify) - 3.5

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

winzip

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

B. No

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

As registered engineers, our Instruments of Service are signed and stamped (or sealed) paper media, and are the only ones that should be relied upon for construction. However, that being said, we recognize that drawings electronically transmitted can accelerate your review and comment time so that approvals can be obtained faster, and we encourge this. We do not electronically transmit our seal nor signature, but your review/comment of a 100% complete drawing set prior to signing and sealing would be beneficial to the building process. We do not believe that the electronic seal and signature transmission process is secure! Note that in most cases we do not provide the sprinkler drawings as the State requires that shop drawings be prepared by a NICET Level III (or better or a registered PE. Thus our design would mostly be redundant, and the building owner does not have to pay twice for the same design.

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 32 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 74.239.90.220
Response Started: Fri, 7/18/08 4:57:00 PM	**Response Modified:** Fri, 7/18/08 4:59:06 PM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

microstation V8XM Audocad

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

B. No

4. What is the largest CAD file size you have ever produced (in megabytes)?

C. 15

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

Outlook

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

No Response

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

No Response

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

PDF format documents is our typical shared document platform

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 31 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 167.7.131.147
Response Started: Fri, 7/18/08 4:42:08 PM	**Response Modified:** Fri, 7/18/08 4:47:52 PM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

We don't produce sprinkler system design drawings, but we use AutoCAD LT 2002.

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

B. 10

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

pkzip

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

B. No

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

B. No

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

We have pdf converter software that may be able to create, transmit and receive electronic signatures, but we have not used that feature.

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 30 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 96.10.99.153
Response Started: Fri, 7/18/08 3:37:57 PM	**Response Modified:** Fri, 7/18/08 3:46:33 PM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

autocad 2008

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

E. 30

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

powerdesk pro - compresses files into zip files.

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

No Response

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

Autodesk Design Review i beleive is a free viewer that handles many different file formats and lets you redline drawings. Please check it out... It would be great to submit plans electronically. I'm not sure what is required for electronic signatures though. I'm sure it shouldn't be a big issue...

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 29 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 129.252.156.137
Response Started: Fri, 7/18/08 3:14:56 PM	**Response Modified:** Fri, 7/18/08 3:23:01 PM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

ACAD

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

No Response

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

winzip

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

B. No

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

OSE is currently considering accepting plans electronically also. Most firms prefer not to send CAD versions of their drawings with seals since it is easy to copy their work and seals from that medium. We have found so far in our investigations that adobe pdf files are the most commonly used for file transfers and also they allow for the use of add on packages for electronic signatures. As you note file size is an impediment and viewing sending and receiving some documents are impossible because of their size. I have reviewed electronic versions of submittals directly on an A/E firms FTP site which eliminates the need for file transfer when they are of a substantial size. The other aspect of electronic review we are investigating is the optimal screen size. If you receive any information on that aspect of electronic reviews, we would love to hear about it. Jim McVey, PE OSE Project Manager jmcvey@mmo.sc.gov 864-503-5534

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 28 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 167.7.126.231
Response Started: Fri, 7/18/08 2:52:21 PM	**Response Modified:** Fri, 7/18/08 3:03:43 PM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

AutoCAD

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

No Response

4. What is the largest CAD file size you have ever produced (in megabytes)?

No Response

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

WinZip

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

No Response

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

No Response

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

No Response

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

No

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 27 of 47 respondents

Response Type: Normal Response
Collector: Survey (Web Link)
Custom Value: *empty*
IP Address: 68.209.89.64
Response Started: Fri, 7/18/08 12:57:23 PM
Response Modified: Fri, 7/18/08 1:00:06 PM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

None

2. Does it allow you to save the design drawings as a .dwg format?

B. No

3. Does it allow you to save the design drawings as a .dwf format?

B. No

4. What is the largest CAD file size you have ever produced (in megabytes)?

Other (please specify) - N/A

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

B. No

6. If so, what software?

N/A

7. Do you have the ability to transmit and receive electronic files?

B. No

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

B. No

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

B. No

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

B. No

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

Unable to send electronically. George H. McCall 864-908-9999

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 26 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 66.35.169.114
Response Started: Thu, 7/17/08 7:04:46 AM	**Response Modified:** Thu, 7/17/08 7:35:37 AM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

AutoCAD 2006

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

D. 20

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

winzip

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

Implement ASAP.

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 25 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 71.75.201.180
Response Started: Thu, 7/17/08 2:03:00 AM	**Response Modified:** Thu, 7/17/08 2:31:12 AM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

AutoCad

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

C. 15

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

Zip. However dwf files are compressed and smaller that pdf's and using the free Design Review from AutoDesk allows you to measure lengths and areas.

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

B. No

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

Depending on the complexity of the drawing (multiple levels, text over-written) it can take longer to review electronically verses paper. Electronic could work well with simple layouts. Others may be easier using prints where you can make notes on the prints. If you go electronic, then you need a plotter to print the ones that are hard to visualize on the screen. Put your hands to your eyes like horse blinders, then hold your eyes 8 to 10in above a print, and move your head around the print. You realize that you need a big screen and a mouse with a scoll button. The equipment will cost money, and it may take longer to review! I would rather see a web site where we could check on the status of our submittals with forecast of review dates that could be accessed via ID and passwords.

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 24 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 66.83.95.170
Response Started: Mon, 7/14/08 9:15:53 AM	**Response Modified:** Mon, 7/14/08 9:25:14 AM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

HYDRATECH

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

D. 20

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

WINZIP

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

NO

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 23 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 70.155.167.76
Response Started: Thu, 7/10/08 5:46:52 PM	**Response Modified:** Thu, 7/10/08 5:49:37 PM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

2004 autocad

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

B. No

4. What is the largest CAD file size you have ever produced (in megabytes)?

D. 20

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

B. No

6. If so, what software?

no

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

I believe this to be a great idea. It lessens the paperwork and gives project managers more time to work rather than run copy after copy

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 22 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 66.35.169.114
Response Started: Thu, 7/10/08 3:28:14 PM	**Response Modified:** Thu, 7/10/08 3:28:55 PM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

autocad

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

D. 20

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

winzip

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

can't wait till this is in place

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 21 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 66.35.169.114
Response Started: Thu, 7/10/08 3:24:28 PM	**Response Modified:** Thu, 7/10/08 3:25:41 PM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

autoCAD 2006

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

D. 20

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

winzip

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

look forward to the implementation of this.

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 20 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 66.35.169.114
Response Started: Thu, 7/10/08 3:22:03 PM	**Response Modified:** Thu, 7/10/08 3:23:36 PM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

autocad 2008

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

E. 30

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

winzip

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

Please implement as soon as possible. Thanks for your assistance.

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 19 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 66.35.169.114
Response Started: Thu, 7/10/08 2:11:32 PM	**Response Modified:** Thu, 7/10/08 2:15:22 PM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

AutoCad 2008

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

D. 20

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

winzip

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

No Thanks

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 18 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 66.35.169.114
Response Started: Thu, 7/10/08 10:15:57 AM	**Response Modified:** Thu, 7/10/08 10:19:59 AM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

HydraCAD

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

D. 20

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

winzip

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

convert to email, much quicker, and save paper

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 17 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 70.155.167.78
Response Started: Thu, 7/10/08 10:02:12 AM	**Response Modified:** Thu, 7/10/08 10:05:57 AM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

auto cad 2004

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

B. 10

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

zip folder

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

no

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 16 of 47 respondents

Response Type: Normal Response
Collector: Survey (Web Link)
Custom Value: *empty*
IP Address: 68.159.67.172
Response Started: Thu, 7/10/08 8:43:58 AM
Response Modified: Thu, 7/10/08 8:59:10 AM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

WE SCAN INTO PDF FORMAT

2. Does it allow you to save the design drawings as a .dwg format?

B. No

3. Does it allow you to save the design drawings as a .dwf format?

B. No

4. What is the largest CAD file size you have ever produced (in megabytes)?

No Response

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

B. No

6. If so, what software?

WE SCAN TO A XEROX 6204 WIDE FORMAT PRINTER

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

B. No

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

B. No

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

ONCE WE RECEIVE SPEC AND COC FROM PE WITH HIS SEAL AND SIGNATURE WE CAN SCAN INTO A FILE ALONG WITH HYDRAULIC CALCULATIONS AND DRAWINGS IN PDF FORMAT AND EMAIL TO LLR FOR REVIEW. WOULD THAT BE ACCEPTABLE? PE THE SIGNATURES ?

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 15 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 68.157.75.215
Response Started: Thu, 7/10/08 8:21:41 AM	**Response Modified:** Thu, 7/10/08 8:23:30 AM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

Hydracad

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

B. 10

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

winzip

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

No

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 14 of 47 respondents

Response Type: Normal Response
Collector: Survey (Web Link)
Custom Value: *empty*
IP Address: 72.242.79.211
Response Started: Thu, 7/10/08 7:55:56 AM
Response Modified: Thu, 7/10/08 7:59:17 AM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

None

2. Does it allow you to save the design drawings as a .dwg format?

B. No

3. Does it allow you to save the design drawings as a .dwf format?

B. No

4. What is the largest CAD file size you have ever produced (in megabytes)?

No Response

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

B. No

6. If so, what software?

none

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

B. No

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

B. No

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

B. No

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

no

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 13 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 66.35.169.114
Response Started: Thu, 7/10/08 7:47:47 AM	**Response Modified:** Thu, 7/10/08 7:50:37 AM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

Hydracad

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

E. 30

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

zip

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

No.

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 12 of 47 respondents

Response Type: Normal Response
Collector: Survey (Web Link)
Custom Value: *empty*
IP Address: 66.35.169.114
Response Started: Thu, 7/10/08 7:47:23 AM
Response Modified: Thu, 7/10/08 7:50:49 AM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

AutoCAD - HydraCAD

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

D. 20

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

No Response

6. If so, what software?

Winzip

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

No thanks.

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 11 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 66.35.169.114
Response Started: Thu, 7/10/08 7:42:10 AM	**Response Modified:** Thu, 7/10/08 7:45:49 AM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

AutoCad

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

No Response

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

winzip

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

none

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 10 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 66.35.169.114
Response Started: Thu, 7/10/08 7:33:22 AM	**Response Modified:** Thu, 7/10/08 7:35:59 AM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

AutoCAD 2008

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

D. 20

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

winzip

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

I believe thie electronic submission on plans will be of great benifit to everyone involved.

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 9 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 74.230.169.203
Response Started: Wed, 7/9/08 8:33:04 PM	**Response Modified:** Wed, 7/9/08 8:41:23 PM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

HydraTec with AutoCAD

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

A. 5

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

Win Zip

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

B. No

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

No.

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 8 of 47 respondents

Response Type: Normal Response
Collector: Survey (Web Link)
Custom Value: *empty*
IP Address: 65.4.67.93
Response Started: Wed, 7/9/08 5:08:27 PM
Response Modified: Wed, 7/9/08 5:13:43 PM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?
AutoCAD w/HydraCAD

2. Does it allow you to save the design drawings as a .dwg format?
A. Yes

3. Does it allow you to save the design drawings as a .dwf format?
A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?
D. 20

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?
A. Yes

6. If so, what software?
PKZIP

7. Do you have the ability to transmit and receive electronic files?
A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?
A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?
A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

I think this would be great.

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 7 of 47 respondents

Response Type: Normal Response
Collector: Survey (Web Link)
Custom Value: *empty*
IP Address: 66.191.213.225
Response Started: Wed, 7/9/08 4:45:33 PM
Response Modified: Wed, 7/9/08 4:48:04 PM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

Autocad 2008, Hydracad

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

E. 30

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

Winzip

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

No

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 6 of 47 respondents

Response Type: Normal Response
Collector: Survey (Web Link)
Custom Value: *empty*
IP Address: 65.44.73.210
Response Started: Thu, 7/3/08 9:27:27 AM
Response Modified: Thu, 7/3/08 9:35:09 AM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?
Autodesk AutoCAD

2. Does it allow you to save the design drawings as a .dwg format?
A. Yes

3. Does it allow you to save the design drawings as a .dwf format?
A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?
A. 5

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?
A. Yes

6. If so, what software?
PK Zip

7. Do you have the ability to transmit and receive electronic files?
A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?
A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?
A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

I work at an architecture office and send out a Ton of paper every month for city review. California for example requires 10 or more signed crimpped sets of documents for review - everyone needing an original signature. I would like to see a single original signature set be issued with a CDROM for plan reviews. Just my thoughts. Roger Fries Property Development GHA Architecture/Development rfries@gha-architects.com

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 5 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 68.216.79.42
Response Started: Wed, 6/18/08 9:21:42 AM	**Response Modified:** Wed, 6/18/08 9:33:44 AM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

Autosprink - Can export to dwg but is not preferred. With Autosprink you can see the entire job in 3D and run calcs instantly.

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

B. No

4. What is the largest CAD file size you have ever produced (in megabytes)?

No Response

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

windows zip files

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

South Carolina has a great setup for the approval process. However, from a contractors' view, it is time consuming for small jobs. In order to meet demanding schedules we NEED a faster way to get drawings approved. The benefits of electronic submittals are tremendous. I am very excited about this. If you need any further comments, please feel free to contact me at jason@ajfire.com. I manage our design department and am the IT manager of our office. I would love to see this happen. Thanks, Jason Johnston Armstrong & Johnston Fire Protection

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 4 of 47 respondents

Response Type: Normal Response	**Collector:** Survey (Web Link)
Custom Value: *empty*	**IP Address:** 96.10.104.89
Response Started: Mon, 6/16/08 9:45:23 AM	**Response Modified:** Mon, 6/16/08 10:25:43 AM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

SprinkCad N1 Autocad Sprinkcad

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

B. No

4. What is the largest CAD file size you have ever produced (in megabytes)?

C. 15

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

WinZip

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

B. No

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

B. No

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

I am all for anything that will speed up the process of getting drawings to your office for review. At this time I am not setup to use electronic seals or signatures. I have not looked into doing this so I am not sure at this time if I can make that change. I will look into it. What I am doing at this time to send drawings to the P.E. for review is I print them to a Adobe .PDF type of file and email those to him for review. There are several programs available that look like a Printer to the cad software. I am using CutePDF Writer at this time.

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 3 of 47 respondents

Response Type: Normal Response
Collector: Survey (Web Link)
Custom Value: *empty*
IP Address: 70.60.221.191
Response Started: Wed, 6/11/08 12:09:43 PM
Response Modified: Wed, 6/11/08 12:18:51 PM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?
Autodesk

2. Does it allow you to save the design drawings as a .dwg format?
A. Yes

3. Does it allow you to save the design drawings as a .dwf format?
No Response

4. What is the largest CAD file size you have ever produced (in megabytes)?
B. 10

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?
A. Yes

6. If so, what software?
BlueBeam

7. Do you have the ability to transmit and receive electronic files?
A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?
A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?
A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

Don't make electronic submission manditory, because not all contractors have CAD software. I also don't appreciate Mr. Galloways comment "Contractors who don't have CAD will have to stepup and get it!" You can tell he has never spent a day in the private sector!!!! Don't create user "mail boxes" for letters - simply e-mail them from Outlook. Don't waste tax dollars inventing a system that is not needed. I don't look forward to having user ID and password to keep up with - I have 4 pages of them for the various systems I have to use. Plus everyone has different rules for how to create a pssword and often to change them!!!!!!!!!!

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 2 of 47 respondents

Response Type: Normal Response
Collector: Survey (Web Link)
Custom Value: *empty*
IP Address: 65.83.197.174
Response Started: Mon, 6/2/08 2:54:53 PM
Response Modified: Mon, 6/2/08 2:57:10 PM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

AutoCAD 2002

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

B. No

4. What is the largest CAD file size you have ever produced (in megabytes)?

A. 5

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

A. Yes

6. If so, what software?

Windows XP

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

B. No

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

B. No

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

None

survey title:
Electronic Sprinkler Plans Submission Survey

current report: Default Report

Displaying 1 of 47 respondents

Response Type: Normal Response
Collector: Survey (Web Link)
Custom Value: *empty*
IP Address: 206.253.150.238
Response Started: Wed, 5/28/08 1:38:52 PM
Response Modified: Wed, 5/28/08 1:40:37 PM

1. What type of CAD software do you currently use for producing sprinkler system design drawings?

Autocad 2008

2. Does it allow you to save the design drawings as a .dwg format?

A. Yes

3. Does it allow you to save the design drawings as a .dwf format?

A. Yes

4. What is the largest CAD file size you have ever produced (in megabytes)?

B. 10

5. Do you use file compression software to decrease the file size of such files (for electronic transmission)?

B. No

6. If so, what software?

N/A

7. Do you have the ability to transmit and receive electronic files?

A. Yes

8. Do you have the ability to transmit and receive sprinkler plans electronically with electronic seals?

A. Yes

9. Do you have the ability to transmit and receive sprinkler plans electronically with electronic signatures?

A. Yes

10. Would you like our office to offer reviews of electronically transmitted documents (instead of paper documents)?

A. Yes

11. Do you have any recommendations (or other comments) for our office to consider regarding this subject?

N/A

Electronic Plan Review E-Mail Submittal Instructions

I. The office of State Fire Marshal now offers electronic plan reviews on all sprinkler projects by e-mail attachment. It is not mandatory, but sending all plan review documents by e-mail is highly recommended. This new process is less expensive, reduces paperwork, simpler and much quicker than printing large sets of documents, packaging them up and sending them by mail or shipping them by express service.

Important Notes:

- Currently, electronic mailing will only be implemented for Fire Protection Sprinkler System Aboveground and Fire Protection Sprinkler System Underground reviews. Other discipline reviews are still be handled by regular mail.

- Before e-mailing a drawing as an attachment, always ensure that the drawing is converted from DWG to a DWF. Newer versions of AutoCAD have the DWG to DWF conversion. If yours does not, you may have to convert to PDF.

- Remember, that all items required to conduct a plan review must be submitted as an attachment in the same e-mail as listed below.

II. Required Documents for Electronic Plan Review

Submit one set of each document specified below by e-mail attachment:

1. **CADD drawing files:** in DWF or PDF format only. (most prefer DWF but not DWG). All drawings must be electronically signed and sealed.
2. **Seismic calculations:** These should be submitted in a PDF format for the sprinkler system.
3. **Hydraulic calculations:** These should be submitted in a PDF format for the sprinkler system.
4. **Certificate of Compliance (COC):** A completed and signed COC should be submitted in PDF format with every project. Please ensure that the COC is completely filled out, signed and sealed by the properly licensed engineer.
5. **Specification Sheet (FSSSS):** A completed and signed FSSSS should be submitted in PDF format with every project. Please ensure that the FSSSS is completely filled out, signed and sealed by the properly licensed engineer. (in PDF)
6. **Manufacturer's cut sheets:** almost always available from vendors as PDF files.
7. Plans that are missing information will delay the review process. Files that have the required information will speed the review process.

South Carolina
Department of Labor, Licensing and Regulation

Division of Fire and Life Safety

141 Monticello Trail
Columbia, SC 29203
(803) 896-9800
FAX: (803) 896-9806 (Fire Marshal)
FAX: (803) 896-9856 (Fire Academy)
www.llr.state.sc.us

Mark Sanford
Governor

Adrienne Riggins Youmans
Director

*****EXAMPLE LETTER*****

November 20, 2008

Crawford Sprinkler Company
Post Office Box 23207
Columbia, SC 29224-3207

Re: Electronic Plan Submittals

Dear Sir or Madam:

In an effort to improve and expedite the plan review process, the Office of State Fire Marshal (OSFM) is pleased to offer a new and exciting service. Effective immediately, the OSFM will offer the option of submitting fire protection sprinkler system plans electronically via an authenticated website.

This new review process will not take precedence over plans that are received via traditional methods (US Mail, FedEx, UPS, etc.), which are still acceptable. However, since our review queue is based on the receive date and processing plans in date order, the electronic plans can get credited with an earlier receive date and therefore receive a corresponding place in the project queue. This new review service will reduce the amount of time that it takes to communicate and process your plans once they are received. There will also be a cost benefit to our customers who can save the costs associated with printing, copying, and delivering traditional paper plans during both submission and resubmission processes.

The OSFM has a website that all electronic plans must be submitted through. This site requires you to have a password in order to submit plans. You will be given a password to access the site. Then once you submit a project, you will be assigned a password that will allow you or designated person to use to upload documents for each project. Once you submit a project and it's plans, they will be logged in, assigned an OSFM project number, and assigned to an engineer for review. All electronic submittals and/or additional information must be received through this website so that they, too, can be logged in and then forwarded to the assigned engineer. Once your plans have been reviewed and a letter has been issued it will be up to you/your company to check your email in order to retrieve your letter. If changes need to be made, you/your company will need to submit the requested changes using the assigned password for the project. Issued letters will remain in your project folder for fifteen (15) days. It will be your responsibility to retrieve your letters within this time as it will also be your responsibility to forward copies of this review to the appropriate persons, including the code officials within the authority having jurisdiction.

Please note that each project needs to be submitted separately. Also note each submittal will have a separate project password. Therefore, it is the responsibility of the submitter to keep track of each project password for each project they submit.

Important Notes:

- Currently, online submission will only be implemented for Fire Protection Sprinkler System Aboveground and Underground Fire Protection Sprinkler System reviews. Other types of plan reviews will still be handled by regular mail.
- Before uploading a drawing as an attachment, always ensure that the drawing file (DWG) is converted to Design Web Format (DWF). [All current versions of Auto Desk products have the DWG to DWF conversion].
- Remember, that all items required to conduct a plan review must be uploaded as listed below. Omission of necessary information will delay the review process.
- For resubmittals, the software will require the use of the project number and password assigned to that project as well as a brief description of the modifications for each resubmittal.
- We reserve the right to request hard copies of plan sets.

Required Documents for Electronic Plan Review: Please upload via the webpage each applicable document in the format specified below: .

1. **CADD drawing files:** DWF format. Each drawing must be electronically signed/sealed.
2. **Seismic calculations:** PDF format.
3. **Hydraulic calculations:** PDF format.
4. **Certificate of Compliance (COC):** PDF format. Completed and electronically signed/sealed.
5. **Specification Sheet (FSSSS):** PDF format. Completed and electronically signed/sealed.
6. **Manufacturer's technical information (i.e. Cut Sheets):** PDF format. Required for specially listed equipment or system components.
7. **Itemized response letter:** PDF format. Only required for resubmittals.

In order to submit plans, you will need to go to http://lookup.llronline.com/fire/login.asp (link for website) and enter the password america. Once at the website, click on the submit plans link and follow the instructions provided. Please note that each field must be filled out or the form will not let you complete to the next step of the process. It is up to **you** as to who within your company has access to submitted project information as you will have to share your project passwords with them. The OSFM will not be responsible for sharing this information with anyone other than the registered customer.

You may reach the Engineering Department's Administrative Assistant at 803-896-9814 with any questions relating to this matter. If you have any questions or need any further assistance, please do not hesitate to contact the OSFM.